An Identity- and Trust-based Computational Model for Privacy

A Thesis Submitted to the
College of Graduate Studies and Research
in Partial Fulfillment of the Requirements
for the degree of Doctor of Philosophy
in the Department of Computer Science
University of Saskatchewan
Saskatoon

By
Mohd M. Anwar

Permission to Use

In presenting this thesis in partial fulfilment of the requirements for a Postgraduate degree from the University of Saskatchewan, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of Saskatchewan in any scholarly use which may be made of any material in my thesis.

Requests for permission to copy or to make other use of material in this thesis in whole or part should be addressed to:

Head of the Department of Computer Science
176 Thorvaldson Building
110 Science Place
University of Saskatchewan
Saskatoon, Saskatchewan
Canada
S7N 5C9

Abstract

The seemingly contradictory need and want of online users for information sharing and privacy has inspired this thesis work. The crux of the problem lies in the fact that a user has inadequate control over the flow (with whom information to be shared), boundary (acceptable usage), and persistence (duration of use) of their personal information. This thesis has built a privacy-preserving information sharing model using context, identity, and trust to manage the flow, boundary, and persistence of disclosed information.

In this vein, privacy is viewed as context-dependent selective disclosures of information. This thesis presents the design, implementation, and analysis of a five-layer Identity and Trust based Model for Privacy (ITMP). Context, trust, and identity are the main building blocks of this model. The application layer identifies the counterparts, the purpose of communication, and the information being sought. The context layer determines the context of a communication episode through identifying the role of a partner and assessing the relationship with the partner. The trust layer combines partner and purpose information with the respective context information to determine the trustworthiness of a purpose and a partner. Given that the purpose and the partner have a known level of trustworthiness, the identity layer constructs a contextual partial identity from the user's complete identity. The presentation layer facilitates in disclosing a set of information that is a subset of the respective partial identity. It also attaches expiration (time-to-live) and usage (purpose-to-live) tags into each piece of information before disclosure.

In this model, roles and relationships are used to adequately capture the notion of context to address privacy. A role is a set of activities assigned to an actor or expected of an actor to perform. For example, an actor in a learner role is expected to be involved in various learning activities, such as attending lectures, participating in a course discussion, appearing in exams, etc. A relationship involves related entities

performing activities involving one another. Interactions between actors can be heavily influenced by roles. For example, in a learning-teaching relationship, both the learner and the teacher are expected to perform their respective roles. The nuances of activities warranted by each role are dictated by individual relationships. For example, two learners seeking help from an instructor are going to present themselves differently.

In this model, trust is realized in two forms: trust in partners and trust of purposes. The first form of trust assesses the trustworthiness of a partner in a given context. For example, a stranger may be considered untrustworthy to be given a home phone number. The second form of trust determines the relevance or justification of a purpose for seeking data in a given context. For example, seeking/providing a social insurance number for the purpose of a membership in a student organization is inappropriate. A known and tested trustee can understandably be re-trusted or re-evaluated based on the personal experience of a trustor. In online settings, however, a software manifestation of a trusted persistent public actor, namely a guarantor, is required to help find a trustee, because we interact with a myriad of actors in a large number of contexts, often with no prior relationships.

The ITMP model is instantiated as a suite of Role- and Relationship-based Identity and Reputation Management (RRIRM) features in iHelp, an e-learning environment in use at the University of Saskatchewan. This thesis presents the results of a two-phase (pilot and larger-scale) user study that illustrates the effectiveness of the RRIRM features and thus the ITMP model in enhancing privacy through identity and trust management in the iHelp Discussion Forum. This research contributes to the understanding of privacy problems along with other competing interests in the online world, as well as to the development of privacy-enhanced communications through understanding context, negotiating identity, and using trust.

Acknowledgements

So many people have helped me in so many ways to make my academic journey thus far. While acknowledging them all, I would like to mention those, who have actively provided me support and encouragement to complete my PhD thesis. In particular, I would like to thank:

Prof. Jim Greer, my advisor, for being a model teacher and researcher and a fine academician from whom I have learned so much, for always challenging me to do my best, for giving me invaluable guidance in pursuing this thesis, and for supporting me both financially and morally.

Azizun, my wife, for being so loving, caring, understanding, and supportive, for trusting in my abilities, for encouraging me to do my best, and for putting up with my workaholic schedule.

Mom and Dad for their unwavering love, support, and encouragement, for teaching me high moral values, and for sacrificing so much to make education the first priority in my life.

Azreen and Tajreean, my daughters, for being delight in my life.

Profs. Gord Mccalla, Simone Ludwig, Julita Vassileva, and Dirk Morrison for serving in my program committee and providing me invaluable advice and encouragement. **Prof. Jacob Slonim** for serving as the external examiner, for doing a thorough review of my thesis, and for challenging me to defend my thesis well.

George Biswas for listening to my ideas and inspiring me, **Ben Daniel** for critiquing my ideas and providing feedback, **Collene Hansen and Chris Brooks** for providing technical support, and all my colleagues at **ARIES lab** for being sociable and friendly. **Lecturer Bryan Puk and students of Introduction to Sociology course** for using privacy-preserving iHelp Discussion tool in their course, and for participating in the post-use survey.

Jan Thompson, Graduate Correspondent, for being a mother figure and a true well-wisher.

This thesis is dedicated to my parents and wife.

Contents

List of Tables

List of Figures

List of Abbreviations

ABAC	Attribute Based Access Control
AC	Access Control
ACL	Access Control List
CA	Certification Authority
CF	Collaborative Filtering
DAC	Discretionary Access Control
FIDIS	Future of Identity in the Information Society
IdP	Identity Provider
ITMP	Identity and Trust based Model for Privacy
MAC	Mandatory Access Control
OM	Obligation Management
P3P	Platform for Privacy Preferences
PDP	Policy Decision Point
PET	Privacy Enhancing Technologies
PGP	Pretty Good Privacy
PIM	Privacy-enhancing Identity Management
RBAC	Role Based Access Control
RPA	Reputation Point Average
PRIME	Privacy and Identity Management for Europe
RRIM	Role- and Relationship-based Identity Management
RRIRM	Role- and Relationship-based Identity and Reputation Management
RT	Reputation Transfer
SAML	Security Assertion Markup Language
SNS	Social Networking Sites
SP	Service Provider
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TMS	Trust Management Systems
XML	eXtensible Markup Language
XACML	eXtensible Access Control Markup Language

Chapter 1

Introduction

We live in the information age: our everyday activities involve sharing torrents of information in a myriad of contexts. Since the Internet has changed the dynamics of our contemporary culture, we have more contexts (from passion to pastime), in which to share information than ever before. Providing easily available media for publications (e.g. blogs, social networks, publishing tools, etc.), the read-only web has transformed into the read-write web. Even though we experience information overload, we record any piece of information that comes our way. Information fusion and data mining techniques allow linking of information from disparate sources despite differing conceptual, contextual and typographical representations. Once collected or captured, our personal information (e.g. our identifying attributes, interests, preferences, and social and economic behaviors) can be used to serve possibly unanticipated purposes (e.g. e-marketing, profiling for personalization or discrimination, publicity or defaming, committing identity fraud, etc.) of the information gatherers resulting in growing concerns over privacy.

Privacy performs a number of important functions for us. Privacy protects us from being misdefined and judged out of context [Cavoukian, 2002]. Privacy is required for personal autonomy, emotional release, self-evaluation, and limited & protected communications [Westin, 1967]. Privacy allows us to make our own decisions, not to be manipulated or exploited by someone knowing our secrets. Privacy provides us "off stage" moments for emotional release when we can be "ourselves": tender, angry, irritable, lustful, or dream-filled. To carry on self-evaluation, privacy is essential. Privacy ensures us limited communication to share confidences and intimacies with those we trust.

Recognizing both the needs for privacy and information sharing, this thesis seeks ways to build a privacy-preserving information sharing paradigm. In this vein, this thesis provides a working definition of information privacy. A comprehensive multi-disciplinary literature review confirms my observation that an individual's expectation of information privacy is contingent on other variables. The amount of privacy individuals seek mostly depends on the context of information sharing, their expectation of security and trust, and their need for information sharing (e.g. personalized services). As a generic solution to privacy-preserving information sharing, an identity and trust-based model for privacy (ITMP) is constructed. The generic ITMP model is instantiated as a Role- and Relationship-based Identity Management (RRIM) solution that is implemented and validated in an e-learning environment. An implementation of RRIM followed by two user studies verify and validate ITMP.

1.1 Problem Statement

Privacy is a notion that is easy to realize, but hard to define. In the literature, privacy is predominantly viewed as users' control over the disclosure of their personal information. However, this notion of privacy does not adequately capture the notion of the control a user needs to experience a desired level of privacy. If a user does not have control over their information beyond disclosure, a piece of their once disclosed information may be inappropriately retained, reused, or repurposed.

Privacy is easy to achieve if there is complete isolation from the rest of the world. But when information sharing is necessary or beneficial, privacy takes on a more complex character. Excessive Privacy may impair the correct assessment of reputation or the offering of personalization. Even though most online users express high privacy concerns, many of them do a striking number of intimate and trusting things online, like personal chat, personal banking, online dating, etc. These privacy-demanding activities underline the need of privacy-preserving reputation assessment, privacy-preserving personalization, or more generally speaking, privacy-preserving information sharing.

The existing privacy solutions look at privacy as a stand-alone notion, and therefore, fail to capture the subtlety of a user's expectation of privacy. Privacy is a subjective and fluid notion. An expectation of privacy is influenced by other needs and expectations. For example, in a trust relationship, an individual's requirement for privacy may be diminished by their expectations of trust. Failing to understand a user's expectation of privacy and variables that influence their expectation results in a solution that cannot offer the subtle variations of privacy that a user seeks. Therefore, a holistic and user-centric solution to privacy in the online world is required. The main problem addressed in this thesis is how to develop and validate a workable, robust, and holistic approach to preserving privacy while allowing for active participation in an online environment.

1.2 Rationale for Conducting this Research

To date, information privacy research has primarily focused on information security, identity management, and policy-based approaches. Security is strongly related to, but not synonymous with privacy: in addition to a secure infrastructure, privacy requires making informed decisions about disclosure. Individuals' controls over their disclosed information are beyond the realm of security. Moreover, state of the art technologies for security require personal information for authentication, and collection and retention of personal information which in itself poses a risk to privacy.

Current identity management solutions do not provide users with control over the usage or the persistence of their disclosed information in the archive-able and searchable online world. Since policy based approaches cannot capture users' diverse and consistently changing needs for privacy, they are ineffective to cater to users' dynamic needs for privacy. This research seeks to advance the research state of the art by progressing to construct a model for privacy that supports selective sharing of information and enables users increased control over their disclosed information.

1.3 General Research Questions

Along with many other researchers, I believe that privacy protection hinges on proper identity management (IM). The primary goal of identity management is to achieve information parsimony (and thereby privacy) by partitioning a user's identity into multiple partial identities according to their participations in various communicative contexts (e.g., my banker needs not know my medical history). Even though identity management is a natural solution to privacy, it is deficient for the following reasons: (i) It cannot adequately restrict the boundary or persistence of disclosed information in the archive-able and searchable online world. For example, once an identity (personal information) of an individual A is revealed to an information seeker B, A's information may be proliferated to yet another information seeker C via B. Also, B may retain information that A once revealed, which was correct at the time of disclosure, but has changed since then. (ii) Reputation earned by one partial identity over time is unusable across other partial identities. For example, when an individual is inducted to a new community with a new partial identity, they cannot use their good reputation earned on existing partial identities of similar contexts.

Privacy is dynamic across individuals, across contexts, and across time. In an interaction, two partners seeking different amount of privacy divulge their identities differently; their need for privacy evolves from one interaction to another. For example, we seek a maximum amount of privacy with total strangers. However, based on positive experience over further interactions (as trusting relationships grow), we may relax the need for privacy. Policy based approaches are not as dynamic as the notion of privacy itself. My research has aimed to build a privacy-preserving information-sharing model that addresses the above-mentioned limitations of existing privacy solutions.

The over-arching goal of this research is to design and validate a privacy-preserving information-sharing paradigm for the online world. Two central research questions emerge from this goal:

- Research Question #1: What key factors need to be considered to holistically

support a privacy-preserving information sharing paradigm?

- Research Question #2: How could one construct and validate a user-centric computational model for privacy, which caters to various information sharing needs, especially as required for personalization in e-learning?

1.4 Scope of this Thesis and Specific Research Questions

These questions delineate a long-term research course that extends well beyond the end of a single thesis. Within this large research area, I have carved out the following set of sub-areas to specifically address in this research: selective disclosure, information expiration, restricting secondary use of information, and reputation transfer. Selective disclosure of information (control over flow) can help users cater to their various information sharing needs without compromising their privacy. Information expiration (control over persistence) and restricting secondary use of information (control over boundary) can help users control the usage of their information beyond disclosure. Reputation transfer resolves the issue of building reputation that arises from preserving privacy by partitioning an identity into multiple contextual partial identities.

In answering research question 1, three factors are identified that can facilitate making information sharing decisions that squarely address privacy concerns: context, identity, and trust. In answering research question 2 using the answer to question 1 (i.e. context, identity, and trust), a 5-layer computational model for privacy (ITMP) is developed to help users make informed decisions regarding what information to share with whom and to control the persistence and boundary of disclosed information so that users' privacy risks are minimized even after disclosure. More specifically, this model supports the following three objectives: (a) restricting flow, boundary and persistence of disclosed information, (b) managing reputation across multiple identities, and (c) personalization. The construction of the ITMP

model leads to the following hypotheses: (i) Understanding and awareness of context contribute to privacy-preserving information sharing, (ii) Identity management contributes to privacy-preserving information sharing, and (iii) Trust can be used to manage privacy. The model is user-centric, because it leverages users' perceived trust towards their partners, and it extends users' control over their disclosed information.

Since information privacy boils down to users' control over their personal information, users should enjoy control over their personal information even after disclosure. My model seeks to enable users to expire their disclosed information or restrict its secondary use by means of making information unusable for the information seekers. Since destroying information is near-impossible (in the archive-able and searchable digital world), disassociating information from its owner makes disclosed information uninteresting and hence unusable. In the Identity and Trust based Model for Privacy (ITMP), a partial identity of information giver is re-crafted for every information-sharing situation resulting in disassociation of previously disclosed information (revealed under a no-longer-existing identifier) from its owner.

Information privacy is a natural concern in the e-learning domain. A large number of e-learning and Web-based intelligent tutoring systems have been developed to perform a variety of tasks related to learning: supporting different learning scenarios (e.g. self-study or guided learning), authoring of learning objects, tutoring, communication, evaluation, annotation, administration, etc. These tasks necessitate that learners in various roles (e.g. student, marker, instructor, peer-helper, etc.) present themselves appropriately and act in line with each others expectations. Through interactions, large amounts of personally identifiable information that could reveal personal details of an actor are transmitted, collected, and processed. Since e-learning is an application domain that comprises many privacy-concerning scenarios representative of those in the online world, e-learning is chosen as a testbed to verify and validate ITMP. ITMP is instantiated as a Role- and Relationship-based Identity Management (RRIM) solution to privacy in the e-learning domain. Consequently, the following domain-specific research questions emerge from the more generic research questions posed in Section 1.3:

- To what extent does RRIM help e-learners maintain their desired amount of privacy while participating in learning activities?

- To what extent does RRIM facilitate trust in a privacy-preserving manner?

Illustrated here is an example scenario of how ITMP may be used in an e-learning environment. A student shares some information in a discussion group under a partial identity with a pseudonym *learner007*. Based on the communicative context and the trustworthiness of the information seeker, the same student may reconstruct a new partial identity under a pseudonym *BobTheWise*. If the student disowns the partial identity of *learner007* leaving no trace to link *learner007* with *BobTheWise*, information released by *learner007* expires and provides no reason for secondary use. Since the ITMP model incorporates trust-based information sharing (use of trust to manage privacy), the model has to facilitate building of users' reputation. In that vein, I developed a trusted public-actor-facilitated, privacy preserving reputation merger protocol across partial identities. Details are provided in RT model in Chapter 3.

1.5 Research Contributions

To help to solve privacy problems in the online world, this thesis makes the following research contributions:

- Introduces a 3-dimensional notion of privacy (Chapter 3). Individuals' privacy is their ability to control the flow, boundary, and persistence of their information.

- Identifies the relationship of privacy with security, trust, and personalization (Chapter 2). Since privacy cannot be achieved without securing users' personal information from unwarranted parties, security is an essential component of privacy. Trust reduces the perceived risks involved in revealing private information. Personalization services require users' willingness to share information, and personalization exposes users to privacy risks.

- Identifies the shortcomings of existing solutions to privacy (Chapter 2).

- Constructs an Identity- and Trust-based model for privacy (ITMP) (Chapter 3). The ITMP model enables privacy-enhanced communications through understanding context, negotiating identity, and using trust. First off, this model constructs a partial identity for an individual by grouping context-relevant information under a transactional identifier or pseudonym and then, in a well understood context, an individual may share some of their identity with a trustworthy information seeker.

- Introduces a reputation transfer (RT) model to enhance the identity management solution to privacy (Chapter 3). Since the pseudo-identities and pseudonyms offered by the identity management solutions are not linkable, reputation earned over a pseudonym is untransferable with the cancellation or switching of that pseudonym. The RT model supports role-specific reputation assessment on a partial identity and allow privacy-preserving reputation transfer among multiple pseudo-identities (e.g. pseudonyms) so that none can draw associations among these pseudo-identities.

- Constructs a Role- and Relationship-based identity Management (RRIM) scheme, a domain-specific instantiation of ITMP. A context can be presented by an assumed role and relationships built by a participant for a specific purpose. In this approach, a role-based identity hides an actor in the crowd of actors with similar roles, and a relationship-based identity allows an actor to disclose limited information appropriate for a respective relationship. Moreover, trusted public roles are assigned guarantor privileges to sanction foul acting and to facilitate usage control over disclosed information.

- Constructs a mechanism for privacy-preserving personalization (Chapter 3). Personalization can adequately be supported by aggregating an individual's behaviours over time in a given context over a persistent identity marker. To support personalization, I suggest the use of sessional tokens to emulate the

effect of persistent markers (shown in Figure 3.8): before the end of each session, a new token will be generated for the next session. If a user chooses to receive a personalized service, the user will present that token at the beginning of the relevant session.

- Introduces the generalized notion of information expiration (Chapter 3). Since the online world lacks the quality of forgetfulness, the privacy threat in the online world is more serious than in the non-online world. Information expiration is achieved through disassociating disclosed information from its owner's pseudonym. Privacy is at risk only when disclosed personal information and the owner (identity) of such information are associable.

- Introduces the concept of identity imprisonment and digital forgiveness to balance privacy and accountability (Chapter 4).The penalty for bad action is being condemned to an identity that cannot be shed. Once an actor is forgiven for some bad actions, they are permitted to acquire a new identity and get a fresh start.

- Implements RRIM in the iHelp online learning environment. A purpose-based and recursive notion of context is identified for the e-learning domain.

- Implements RT model and validated the model through simulation and human expert study. A prototypical system has been built that manages reputation for three different sorts of roles present in an e-learning community: helper, peer, and lurker. A study was designed to see whether our system facilitates reputation based trust while preserving privacy by making secure reputation transfer/merge across multiple pseudonyms. Results confirm that the system supports reputation transfer with privacy preservation.

- Conducts a pilot and a large-scale research study to test the effectiveness (usability and functionalities) of RRIM to offer privacy-enhanced learning environment. The analysis of usage data and user survey data shows that the system

provides users with control over the choice and disclosure of their identity and awareness of their identity and behavior.

1.6 Organization of the Thesis

Chapter 2 surveys existing works in privacy and in related areas like security, trust, and personalization that affect privacy, particularly in e-learning environment. Chapter 2 also surveys issues of privacy, security, trust, and personalization in e-learning environments, which is later used as a testbed for testing the proposed solution to privacy. Chapter 3 presents a 5-layer Identity and Trust based Model for Privacy (ITMP). As an integral part of the ITMP, a reputation transfer (RT) model is also presented in Chapter 3. Chapter 4 describes the implementation of a Role- and Relationship-bases Identity Management (RRIM) model, an instantiation of the generic ITMP model. Chapter 4 also reports a stand-alone implementation of the RT model. Chapter 5 reports the verification and validation of RRIM (and thereby, the verification and validation of ITMP) and the RT models. Chapter 6 concludes this thesis by summarizing the work done in the thesis and presenting research contributions and future work.

Chapter 2

Related Work

"Privacy, like an elephant, is ... more readily recognized than described" [Young, 1978]. Due to its highly nuanced and context-dependent nature, privacy is hard to define [Patil and Kobsa, 2005]. It has been investigated along many dimensions (e.g. social, technological, legal, philosophical, etc.) by multiple disciplines. Extrapolating from the findings of this chapter leads to this thesis work that addresses issues of privacy through understanding context, negotiating identity, and using trust. This chapter reviews works on privacy, security, trust, personalization, and e-learning that have inspired this thesis. To treat the issues of privacy squarely, this research studies privacy together with other variables that positively or negatively influence privacy concerns. For more focused analysis, in this chapter, privacy is investigated in the e-learning domain, where the need for information sharing is as important as privacy.

2.1 Information Privacy

Probably, the first publication advocating privacy was the article by Judges Warren and Brandeis, in which privacy is termed as "the right to be let alone," and in their opinion, "the right most valued by all civilized men" [Warren and Brandeis, 1890]. From then on, researchers, companies, and governments have focused on addressing privacy issues through policies, technologies, legislation, and privacy impact assessments, and still they do not seem to be adequate. With the advent of the Internet, the World Wide Web, and Web 2.0, privacy took on a new dimension. This chapter tries to capture this incarnation of privacy, to be precise, information privacy.

Privacy is a multi-dimensional concept: it is perceived as various things ranging from solitude [Brierley-Newell, 1998], to control [Gavison, 1984], to un-observability [Altman and Chemers, 1980], to access control, data integrity and identity management [Sweeney, 2002], etc. However, as Solove puts it,"these abstract incantations are not nuanced enough to capture the problems involved" [Solove, 2006]. A fuller analysis of privacy merits examining various cross-disciplinary privacy literature.

Traditional approaches understand privacy as a state of social withdrawal [Palen and Dourish, 2003], which is quite undesirable in today's information society. Instead, social psychologist Irwin Altman's observations on how people manage face-to-face interaction seem more relevant to privacy in our information society. Altman conceptualizes privacy as a boundary regulation process, where people optimize their accessibility along a spectrum of "openness" and "closedness" depending on a context [Altman, 1975]. According to Dourish and Anderson, flows of information serve as markers of social boundaries, providing a means to negotiate, demonstrate, and sustain patterns of identity, membership, and affiliation in social groups [Dourish and Anderson, 2006]. The goal of privacy is to achieve the desired state along the spectrum of openness and closedness. Therefore, in Altman's view, privacy is not simply a matter of avoiding information disclosure, but rather, context-dependent selective disclosure of personal information.

The concerns over privacy seek a necessary balance between privacy and publicity. This balance can be achieved through maintaining the contextual integrity of information. Information is only sensitive (or not) relative to the context and rules governing the flow of information from one party to another depending on the nature of context [Nissenbaum, 2004]. Nissenbaum posits that contextual integrity is maintained when both the "appropriateness" and "distribution" norms of information are upheld. The appropriateness norm dictates what information about a person is appropriate to reveal in a particular context. For example, in a medical context, it is appropriate to share details of our physical condition with the physician but not vice versa. The distribution norm regulates the flow or distribution of information appropriate in a particular context. For example, in a friendship context, free choice,

discretion, and confidentiality are the prominent norms of distribution.

Putting control in the hands of the stakeholders, privacy is defined as claims or ability of individuals to control the collection, retention, and distribution of information about themselves [Westin, 1967, Goldberg et al., 1997]. Many privacy principles, policies and regulations like the Personal Information Protection and Electronic Documents Act (PIPEDA) [Department of Justice, 2000] of Canada, ACM recommendations [USACM, 2006], and EC Directives on the protection of personal data [EU, 2002] are in line with this notion of privacy. However, who has the rights about which information could be a convoluted question. This challenge is echoed in the privacy definition given by economist Eli Noam [Noam, 1997]: "Privacy, by definition, is an interaction in which the informational rights of different parties collide. Different parties have different preferences on "information permeability" ..."

Today, some unseen parties on the Internet can monitor almost all online e-services. The controversies about cookies, click streams, traffic analysis, packet sniffing, and spam form merely the tip of an iceberg. Lessig's notion of privacy reflects on this inherent nature of the digital world. He projected that we are fast entering an age where more can be known and more efficiently collected than at any time in our history. Lessig, a legal scholar, suggests that we think of privacy as a function of the monitored and the searchable [Lessig, 1999]. Grudin also observes that knowing that any digital information we generate will likely be stored and indexed transforms how we communicate and present ourselves [Grudin, 2001].

Goffman's observations that individuals reveal and conceal information selectively to maintain context-specific identity and social relationships [Goffman, 1959] set the stage to think about privacy in terms of identity. Rao and Rohtagi view privacy as the right of individuals to protect their ability to reveal information selectively about themselves so as to negotiate social relationships most advantageous to them [Rao and Rohatgi, 2000]. Demchak and Fenstermacher note that privacy is directly related to the knowledge of identity [Demchak and Fenstermacher, 2004]. A similar notion of privacy is manifested in the work of both Samarati and Sweeney [Samarati, 2001, Sweeney, 2002]. A general doctrine of their works is to release all

the information, but to do so such that the identities of the people who are the subjects of the data (or other sensitive properties found in the data) are protected.

2.1.1 Privacy Solutions

Song et al. effectively define the process of privacy protection - it is a process of finding an appropriate balance between privacy and multiple competing interests [Song et al., 2006]. In this regard, personalization, security, and trust are viewed as competing interests to privacy. From a business perspective, privacy is important for making consumers comfortable disclosing the personal information needed for marketing relationships [Culnan, 2000]. Since the disclosure of personal information is the crux of the privacy matter, it is critical to find an unambiguous definition of personal information. Under Canada's Personal Information Protection and Electronic Documents Act, PIPEDA, "Personal Information" means any information that is uniquely connected with an individual, including name, address, telephone number, social insurance number, and date of birth. It also includes, but is not limited to, other information relating to identity, such as, nationality, gender, marital status, financial information, and credit history (PIPEDA, 2003).

Al-Fedaghi provides a more formal definition of personal information: personal information (PI) is any linguistic expression that has referent(s) of type, person [Al-Fedaghi, 2005]. Assuming that p is a sentence such that X is the set of its referents, and then there are two types of PI:

- p is atomic personal information if it is an assertion that has a single human referent (e.g., John is 25 years old). Here, "Referent" implies an identifiable (natural) person.

- p is compound personal information, if it is an expression that has more than one human referent (e.g., John loves Mary).

However, this definition includes observation, reputation, or even public information in the realm of personal information, and thereby, may introduce more ambiguity. For example, information referring to John in his professional capacity as mayor, for

example, should not be considered as his personal information. My thesis addresses this shortcoming by considering context in determining personal information.

Personal information may be any of many items, including an individual's shopping habits, nationality, work history, living habits, personal communications, email address, IP address, physical address, identity, and others. The use of one's true and complete identity makes personal data collection very easy and efficient through integration, interconnection, and data mining technologies. Digital identities (i.e. a set of claims made by one digital subject about itself or another digital subject." [Cameron, 2005]) and profiles are getting more and more relevant to enable Internet transactions and interactions among the citizens; they are precious for personalization, but any kind of misuse causes violation of privacy, fraud, etc. [Mont et al., 2003]. Therefore, it is believed that mechanisms such as anonymity and pseudonymity are the essential building blocks in formulating solutions to privacy protection [Rao and Rohatgi, 2000], and a considerable amount of effort has been devoted towards realizing these primitives in practice.

Anonymity refers to the ability of an individual to perform a single interaction with another entity (or a set of entities), without leaking any information about their identity. Kobsa and Schreck talk about different types (i.e., Environmental, Content based, and Procedural) and levels of anonymity [Kobsa and Schreck, 2003]. Environmental anonymity states that the people of one's direct environment must not disclose the identity of a person who wants to act anonymously. Content-based anonymity is maintained when the identity cannot be deduced from the user or documentation data. Procedural anonymity is maintained when the recipient of the message cannot identify the sender of a message and vice versa.

In Windley's view [Windley, 2005], in a circular manner, privacy is built upon a foundation of good information security, which is dependent upon good identity management. He further suggests that digital identity management should be built on the following set of concepts: integrity and non-repudiation, confidentiality, authentication and authorization, identity provisioning, and representing & managing authorization policy [Windley, 2005]. These above mentioned concepts can be im-

plemented by existing technologies. Digital signatures ensure message integrity and prevent a signer from repudiating a message. Encryption infrastructure like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) can provide confidentiality. SAML (Security Assertion Markup Language) [Cantor et al., 2005] allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject to other entities, such as a partner company or another enterprise application. Provisioning is the creation of an identity record and its population with the correct attributes. SPML (Service Provisioning Markup Language) provides a standard XML format for exchanging provisioning requests and responses. The eXtensible Access Control Mark-up Language, or XACML, attempts to solve the authorization problem by providing an XML-based language for storing and sharing access control policies. However, these privacy-enhancing tools do not help users in making an informed choice about to whom to share what piece of their personal information for what purpose, neither does it help users in choosing an appropriate identity for a given context. My thesis addresses privacy enhancement through enabling users to make informed choices about disclosure of their personal information.

Palen and Dourish describe three interrelated boundaries for privacy management: disclosure, temporal, and identity [Palen and Dourish, 2003]. Depending on the context, public and private are continuously refined between these boundaries. Users would like to be able to control an appropriate level of content sensitivity given the context of viewing (disclosure boundary). The persistence of traces of the previous activities (temporal boundary) makes it difficult for users to ensure that they are presenting themselves appropriately for their current role (identity boundary). The tools of self-awareness and identity management capabilities can maintain the above-mentioned privacy boundaries. An identity management system should be able to help users to select among the anonymous, pseudonymous, or identified interactions and help them maintain the underlying identity [Borcea et al., 2005].

As part of a solution to privacy, in her Masters thesis [Boyd, 2002], Boyd argues for empowering the users through awareness and control. Contextual understanding and personal self-awareness are the building blocks that people use to properly con-

trol their identity and presentation during their social interactions. Self-awareness allows users to understand who they are in a particular environment, how the facets of their identity are manifested and aggregated, how other people and sites can see them. Recent privacy enhanced technologies (PETs) are aimed at empowering users in their privacy decisions [Wang and Kobsa, 2008]. Donath also emphasizes the need for self-awareness to protect an individual's privacy. The content of an interaction can reveal a great deal about the interactor, which may include explicit identity attributes (e.g. name, age, and sex) [Donath, 1998]. Identity management tools aim to provide users with a desired control over their presentations.

PRIME's (Privacy and Identity Management in Europe) vision is to give individuals sovereignty over their personal data so that [Camenisch et al., 2005]: Individuals can limit the information collected about them, negotiate legally-binding "privacy policies" with their service providers, use automated mechanisms to manage their personal data and their obligations towards data that they have collected from other parties. Users can apply privacy enhancing identity management (PIM) in order to control which info they disclose to whom in which situation [Franz et al., 2006]. In a representative PIM system developed by PRIME, a database holds certificates and declarations of a party which is guarded by an Access Control component (AC). An Identity Control (IC) and a graphical user interface (GUI) facilitate the overall privacy and identity management task. In addition, service providers will also have an Obligation Management component (OM) which manages all of the privacy obligations the company has assumed regarding the collected data [Mont, 2004].

The PRIME model for privacy uses privacy enhancing identity management to provide users with control over the disclosure of their personal information. Even though identity management helps users to limit the disclosure of their personal information through enabling them to partition their identity into different partial identities based on their vague understanding of context, it does not provide any mechanism for users to fully understand and differentiate contexts. Moreover, partitioning of identity, as done in PIM, is an unattractive solution to privacy due to the fact that good reputation earned under one partial identity is unusable in another

partial identity. The PRIME model does not address the dynamic need for privacy: the need for privacy evolves as actions of one actor are continuously screened by another actor resulting in changing measures of trustworthiness. In this searchable and archive-able online world, where information from disparate sources can easily be fused, users need control over the usage of their personal information. The PRIME model tries to achieve that control by ensuring the information seeker operates under legally binding privacy-policies. Since legally binding privacy policies cannot adapt to the dynamic nature of privacy needs, this model cannot provide users with adequate control over their personal information after disclosure. Privacy concerns arising from the persistent nature of disclosed information can be addressed by enabling users to make their personal information unusable in the future as need be. The PRIME model does not address this type of privacy concerns. My thesis addresses these shortcomings of PRIME's identity management-based solution to privacy.

When identity management solutions to privacy are becoming prominent, decentralized identity systems, known as OpenID, are increasingly providing personal identity to online users. Eliminating the need for remembering a lot of different passwords for different sites, a user signs in to their openid identity provider (IdP). As an authentication broker, the OpenID IdP authenticates the user to a relying website (of IdP). Recordon and Reed group OpenID systems into two categories [Recordon and Reed, 2006]: (1) Address-based identity (uses a digital address to identify users) and (2) Card-based identity(uses a digital token to references a collection of claims). OpenID enables users to use a single URI-based identity (e.g. http://alice.openid-example.org/) to log into multiple web sites. Even though decentralized identity systems give individuals more control over how they express their own identities [Weitzner, 2007], which is important for privacy-enhanced information sharing, OpenID poses certain privacy risks [Recordon and Reed, 2006]: (a) an OpenID provider will know every web site a user logs into with OpenID (b) if an impostor gains access to a user's OpenID account, they will be able to navigate into all of that user's different OpenID-enabled sites. In essence, OpenID is more

concerned with scalability than security [Maler and Reed, 2008]. In a study of how to provide trust, safety and privacy to online users, Kim Cameron, chief identity and access architect at Microsoft, identifies the underlying problems with the Internet [Cameron, 2005]: the Internet was built without a way to know to whom and what one is connecting. He develops a formal understanding of the dynamics causing digital identity systems to succeed or fail in various contexts and expressed them as the "Laws of Identity" (described below) [Cameron, 2005]. These quoted descriptions below are taken from Cameron, 2005, pages 5-9.

1. User Control and Consent: Identity systems must not disclose a user's identifying information without their consents. "The system must also protect the users against deception, verifying the identity of any parties who ask for information." ... "It must reinforce the sense that the user is in control regardless of context ..."

2. Minimal Disclosure for a Constrained Use: Identity systems should reveal as least amount of identifying information as possible. "The concept of "least identifying information" should be taken as meaning not only the fewest number of claims, but also the information that is least likely to identify a given individual across multiple contexts. For example, if a scenario requires a proof of a user being of a certain age, then it is better to acquire and store the age category rather than the birth date." The system should acquire and retain information only on a need basis.

3. Justifiable Parties: "Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. The identity system must make its users aware of the party or parties with whom they are interacting while sharing information." Since Microsoft did not have a justifiable relationship with the customers of non-MSN sites, Microsoft Passport failed to be an identity system

for the Internet.

4. Directed Identity: "A universal identity system must support both "omni-directional" identifiers for use by public entities and "uni-directional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles." ... "A consumer visiting a corporate Web site (public entity) is able to use the omni-directional identity of that site to decide whether she wants to establish a relationship with it. Her system (private entity) can then set up a "unidirectional" identity relation with the site by selecting an identifier for use with that site and no other."

5. Pluralism of Operators and Technologies: "A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers." A device driver or a network socket like unified interface is required for interoperability.

6. Human Integration: "The universal identity meta-system must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks." ... "The identity system must extend to and integrate the human users." Human integration and rich user experience contribute to predictable and unambiguous communication.

7. Experience across Contexts: "The unifying identity meta-system must guarantee its users a simple and consistent experience, while enabling separation of contexts through multiple operators and technologies." "Let's project ourselves into a future where we have a number of contextual identity choices. For example:"

    - "Browsing: a self-asserted identity for exploring the Web (giving away no real data)"
    - "Personal: a self-asserted identity for sites with which a user wants an ongoing but private relationship"

- "Community: a public identity for collaborating with others"
- "Citizen: an identity issued by the government"

Based upon the "Laws of Identity" ([Cameron, 2005]) and extending the concept of address-based OpenID, Microsoft proposed a card-based identity system, namely Cardspace. A card-based identity can contain one or more address-based identities. Cardspace implements the "Information Card model", which refers to the use of Information Cards containing metadata for obtaining digital identity claims from identity providers (e.g. Windows Live ID can be one of multiple such identity providers) and then conveying them to relying parties under user control [Nanda, 2007]. Residing at the client platform, the information cards provide visual representations of digital identities for the end user. Users may decide to release tokens (containing requested information) based on the service provider's privacy policy. No assumptions are made regarding the format and content of the privacy policy, and an identity selector (a module in cardspace) is not required to parse, interpret or act on the privacy policy programmatically [Nanda, 2007].

Even though no explicit communication between an Identity Provider (IdP) and a service provider (SP) is expected in this model, an identity provider has an option to identify the relying party, where the token will be used. As a result, an IdP can follow a user's activity trail. Jøsang et al. observe that Kim Cameron's 3rd law of identity (i.e. Justifiable Parties) still applies to Cardspace. It is unacceptable from a privacy perspective to entrust third parties with personal information when they have no direct involvement in the relationship between the user and the SP [Jøsang et al., 2007]. An attacker can steal authentication tokens for accessing IdPs in the same way as passwords are stolen from a client platform, e.g. through phishing or Trojans. With a stolen InfoCard, the attacker is able to access an user's services without the user's knowledge.

Cardspace lets users choose a different InfoCard for each different context. However, the system does not help users understand different contexts or choose a context-appropriate InfoCard. This limitation is addressed in my thesis. In Cardspace,

trust is defined as the willingness of a subject to believe the claims asserted by a certain other subjects. For example, Verisign (a trust provider) asserts, via a certificate, that this SP website is the real xyz.com (not a phishing site). However, with this information, a user will not be able to make a trust-based privacy decision. A user needs to know if the SP has a good reputation for protecting collected information or if the SP has a good reputation for not repurposing collected information. The ITMP model of my thesis helps users to make a trust-based privacy decision.

Lorrie Cranor (author of P3P) broadly categorizes the technologies for realizing privacy into three different categories [Cranor, 1999]:

1. Anonymizing Agents - ensure that packets from a user cannot be linked to their identifiable IP address. Examples of such technologies include Anonymizer [1], Crowds [Reiter and Rubin, 1999], Onion Routing [Goldschlag et al., 1999] and the IP Wormhole technology of the Freedom network [Goldberg and Shostack, 2001].

2. Pseudonym Agents - manage pseudonyms in order to develop persistent but unidentifiable relationships. Lucent Personalized Web Assistant (LPWA) [Gabber et al., 1999] or Freedom Network's NymSrv are examples of pseudonym agents.

3. Negotiation Agents/Trust Engines - negotiate on a user's behalf and determine when a user's privacy policies are satisfied. The TRUSTe [2] is an example of a trust engine in which Web sites can be licensed to display a privacy seal or trust-mark on their sites.

Rao and Rohatgi mention another category of technologies for preserving privacy, called application level filters, that eliminate obvious identity information from an individual's web traffic, such as name, e–mail address, affiliation, etc.
[Rao and Rohatgi, 2000]. Examples of Application level filters include the Freedom word scanner [Goldberg and Shostack, 2001].

[1] http://www.anonymizer.com/
[2] www.truste.org/

Wang and Kobsa group Privacy Enhancing Technologies (PETs) into the following three categories [Wang and Kobsa, 2008]. These quoted descriptions below are taken from Wang and Kobsa, 2008, page 207.

- Protection of identity: "this type of privacy protection aims to prevent users' true identities from being revealed (i.e., who they are)." Cardspace and Anonymizer are examples of PETs, which are partially effective in providing this type of privacy protection.

- Seclusion: "this type of privacy protection attempts to prevent users from being bothered by unwanted contact or solicitation (e.g., spam emails)." Privacy Bird, Popup Blockers, or Anti-spams softwares are examples of PETs, which provide this type of privacy protection.

- Control over data: "this type of privacy protection allows users to have control over their data, e.g. regarding what data can be collected or disclosed for what purpose, how the data will be used, and with whom the data may be shared or to whom it may be transferred." PGP, Privacy Bird, Cardspace, OpenID are examples of PETs, which provide this type of privacy protection.

Education and awareness can also contribute to privacy protection. For example, adults are concerned about invasion of privacy, while teens freely give up personal information. This occurs because often teens are not aware of the public nature of the Internet or cannot foresee the consequences [Barnes, 2006]. Holtzman lays out what he describes as the "Seven Sins" against privacy [Holtzman, 2006]: intrusion, latency, deception, profiling, identity theft, outing, lost dignity. Patil and Kobsa identify the following principles and factors, which seem to influence privacy management in collaborative work settings [Patil and Kobsa, 2003]: reciprocity, feedback, context, control, norms, inference, overhead, incentives, conflicts, archiving.

Other surveyed solutions to privacy include cost-benefit analysis model, anonymization techniques, and trust building between information sharing partners. Acquisti points out that people sometime ignore privacy risks in the temptation of immediate gratification [Acquisti, 2004]. In the cost-benefit analysis model of Buffet et al., the

request for personal information is only acceptable when the user's perceived value is comparable to the offered reward, and the reward outweighs any privacy risk to personal information [Buffett et al., 2004]. The sets of attributes (like gender, date of birth, and zip code) that can be linked with external data to uniquely identify individuals in the population are called quasi-identifiers [Dalenius, 1986]. To counter linking attacks using quasi-identifiers, Samarati and Sweeney propose a data anonymization technique called k-anonymity ([Samarati, 2001]; [Sweeney, 2002]). The idea is to hide in a crowd of size k so that the chance of getting uniquely identified decreases. Machanavajjhala et al. show that k-anonymity cannot protect individuals from being identified due to lack of diversity in their sensitive attributes and propose l-diversity (i.e. each k-anonymous group should have at least l distinct sensitive values) to enhance k-anonymity [Machanavajjhala et al., 2007]. Agrawal et al. propose anonymization through perturbation of data from multiple clients before integrating at the server in order to preserve privacy [Agrawal et al., 2005]. Wu and Weaver propose a trust building mechanism that discloses only the attributes of the clients required to negotiate a trust relationship, thereby preserving the clients' privacy [Wu and Weaver, 2005]. After the trust negotiation is successful and trust has been established, the clients use dynamic validation to monitor and maintain their trust relationships.

Privacy is a fluid concept, which has evolved into a notion that realizes the need for information sharing. This thesis does not view privacy as absolute seclusion, but selective disclosure (users' right to negotiate their identity in multiple contexts by controlling the flow of their personal information). The goal of privacy is to achieve the desired state along the spectrum of openness and closedness. Therefore, as in Altman's view, privacy is not simply a matter of avoiding information disclosure, but rather, context-dependent selective disclosure of personal information.

According to the findings of the reviewed literature, information privacy research has primarily focused on information security, identity management, and policy based approaches. Security is strongly related, but not synonymous to privacy: in addition to a secure infrastructure, privacy requires making informed decisions about

disclosure. Even though identity management limits disclosure by partitioning an identity into many partial identities for each of the user defined contexts, it does not provide users with control over the usage or the persistence of their disclosed information in the archive-able and searchable online world. Since policy based approaches cannot capture users' diverse and consistently changing needs for privacy, they are ineffective to cater to users' dynamic needs for privacy.

2.2 Security as it Relates to Privacy and Identity

In the computer industry, security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization [3]. Security reduces our risks of exposure and protects the organization's assets, such as client information, intellectual property, strategic goals, and financial statements [Cady and McGregor, 2002]. Most security systems are identity-based schemes [White, 2004] that mainly focus on how to identify a user and what type of access right should be given to the user. El-khatib et al. state the following roles of security [El-Khatib et al., 2003]: user authentication /authorization, protection of private information from unintended access, and protection of data integrity (guarding against data corruption by attackers).

Security for e-services has been a major requirement for their acceptance, and providing an acceptable level of security has been a difficult problem ([Joshi et al., 2001]; [Rust and Kannan, 2003]). Security is not a fixed objective to achieve, but rather, a process that is always evolving as the businesses change. Ellison and Schneier assess that security is very difficult, both to understand and to implement
[Ellison and Schneier, 2000]. The necessary key functions of security are access control and protection of resources, which are addressed by deploying authentication systems.

The complexity of the interplay between authentication and privacy becomes clear when one tries to define authentication, which can take multiple forms

[3] www.webopedia.com

[Kent and Millett, 2003]:

- "Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual."
- "Identity authentication is the process of establishing an understood level of confidence that an identifier refers to an identity. The authenticated identity may or may not be linkable to an individual."
- "Attribute authentication is the process of establishing an understood level of confidence that an attribute applies to a specific individual."

The three generic means of authentication that tend to be used in practice [Kent and Millett, 2003] can be described loosely as: i) "something a user knows" - e.g. a password or passphrase, ii) "something a user has" - e.g. ID card or security token, or iii) "something a user is" - e.g. a biometric identifier. However, from privacy perspectives, it is important to understand what kind of security is necessary, and is authentication required? When required, which types of authentication might serve best? For example, individual authentication may be necessary when accountability is required; otherwise, attribute authentication (or no authentication) may suffice. Users also need to authenticate the service providers to ensure that their own personal information does not fall into the wrong hands. Service providers usually use certificates to proclaim their identities.

Bashir et al. describe access control as a process by which the use of the system resources is regulated according to a security policy and is permitted by only the authorized entities (users, programs, processes, or other systems) according to that policy [Bashir et al., 2001]. In general, the three major access control models are identified in the literature: mandatory access control (MAC) [Bell and Padula, 1976], discretionary access control (DAC) [Ventuneac et al., 2003], and role-based access control (RBAC) [Barkley et al., 1997]. In the MAC model, the user's access to a certain resource is permitted only if the user's access level matches the sensitivity level assigned to the resource. In the DAC model, the creator of a resource decides who will have access to the resource, and what related operations are allowed. In

RBAC, a subject can access resources based on their assigned roles, conforming to the privileges granted to the respective corresponding role. The Attribute Based Access Control (ABAC) model is the newest of the listed four approaches.

ABAC supports both the mandatory and the discretionary access control needs [Yuan and Tong, 2005]. In ABAC, a requester is granted access to a collection of services based on a furnished collection of attributes. For example, in mandatory access control, the clearance labels of a subject are considered as subject attributes and objects' classification labels as object attributes. An authorization process, then, evaluates the dominance of these labels along with the requested access rights (e.g., read, write) to return either 'allowed' or 'not-allowed'. Similarly, in discretionary access control, an access control list (ACL) can be viewed as object attributes and a capability list as subject attributes. The ABAC decisions are made based on the requesters attributes, which are demonstrated through the disclosure of digital credentials. Using pseudonyms, such credential systems allow users to prove their attributes (e.g., age, zip code, etc.) without disclosing their identities.

An access control policy simply states, "who can do what to what"[Merrells, 2004]. The who is a subject, the first what is an action, and the other what is a resource. A rule can have the effect of either permitting or denying access. The rule is constrained to the specific subject, resource, and action by the contents of the Subjects, Resources, and Actions elements. The component that processes the policy is called the Policy Decision Point, or PDP. The PDP accepts access control requests, processes them against the policy and returns an access control response. XACML is an example of an access-control policy language.

The Internet infrastructure could not be secured without implementing some technological controls, such as firewalls, anti-virus, anti-spyware, and anti-spam software, encryption, operating system hardening, intrusion detection systems, and vulnerability scanning. Menard suggests three basic steps for good security [Menard, 2006]: (i) Know and understand what needs to be protected, (ii) Think about security as a process, which is always evolving, always changing, and (iii) Think about security in terms of technical and non-technical layers complementing each other.

Since privacy cannot be achieved without securing users' personal information from unwarranted parties, security is an essential component of privacy. However, social engineering attacks are the manifestation of the fact that identification of unwarranted parties goes beyond the realm of security. Posing risks to privacy, many security enforcing mechanisms collect personal information of users for authentication. Therefore, an ideal security solution has to protect personal information that is collected by its authentication system. Moreover, personal information has to be protected against being repurposed, which cannot be achieved by means of security.

2.3 Trust as it Relates to Privacy and Identity

Trust is a word that people constantly use to mean different things in different circumstances, and in different scenarios (e.g. trust among parties, trust in the underlying infrastructure, etc.). Wang and Vassileva observe the context-specific, multifaceted, and dynamic nature of trust [Wang and Vassileva, 2003]. The American heritage dictionary defines trust as 'firm reliance on the integrity, ability, and character of a person or thing.' According to Handy, trust is "a confidence in someone's competence and his or her commitment to a goal" [Handy, 1999]. Luhmann views trust as the choice to expose oneself to a risk toward one's counterpart, in the expectation that the counterpart will not disappoint such expectation [Luhmann, 2000].

Trust can be seen as a complex predictor of an entity's future behavior based on past evidence. Just as we would deliberate whether or not we could trust someone with our valuables, it is also crucial to calculate the trustworthiness of actors to decide what piece of information would be safe with them and in what context. Building up mutual trust is important for every communicative context. If trust is not present in a relationship, a large amount of energy is wasted in checking up on the other's commitments.

Use of trust is often implicit. A user who downloads a file from an unfamiliar web site trusts the web site implicitly, not considering trust consciously. Trust may be built offline for the online activities, by asking friends for recommendations. Without

trust, the Internet will not be able to realize its full potential. The two important factors that are known to build trust in online business transactions are the consumers' familiarity with the vendors [Sheehan and Hoy, 2000], and consumers' experiences with them [Doney and Cannon, 1997]. To make this past experience positive, information about an individual needs to be handled in a way that is consistent with the privacy and security expectations of the individual – if not, there will be no trust [Patrick, 2002].

Reputation is more of a social notion of trust [Golbeck and Hendler, 2004]. In our lives, we each maintain a set of reputations for the people we know. When we need to work with a new, unknown person, we can ask people with whom we already have relationships for information about that person. Based on the information we gather, we form an opinion about the reputation of the new person. This system works well, even though there are many people in the world, because communities tend to be highly interconnected, and the number of steps between any two people tends to be rather small. This is known as the Small World effect, and it has been shown to be true for a variety of social and web-based systems [Adamic, 1999].

Though trust can be based upon many different sources (e.g. social rules, professional ethics, legal rules, etc.), reputation is the most effective source for measuring trust online. Sartor states that reputation results from shared beliefs, which spread in a society as a consequence of complex social interactions [Sartor, 2006]. Individuals form opinions concerning a certain person (based on personal experience or of certain indexes), they convey such opinions (person X is . . .) or their beliefs about others' opinions (it is said that person X is . . .), these opinions and beliefs are adopted by others and further conveyed. In the real world, trust is developed through day-to-day activities where everyone gets to see and know one another on a regular basis. By contrast, in the online world, trust relationships are developed among entities, who are mostly strangers, based on their longitudinal social behaviors.

Marsh addresses the issue of formalizing trust as a computational concept in his PhD dissertation [Marsh, 1994]. In his model, trust is treated as a subjective and mathematical entity, and it is computed using a subjective real number arbitrarily

ranging from -1 (complete distrust) to +1 (blind trust). In the work of Goldbeck and Hendler, trust is treated as a measure of uncertainty in a person or a resource [Golbeck and Hendler, 2004]. Specifically, having trust in a person is defined as a measure of the confidence that the person will take the action that leads to the positive result. In both of the models ([Marsh, 1994]; [Golbeck and Hendler, 2004]), reputation is synonymous with the measure of that trust.

The issue of trust and reputation on the web has been around since the web itself began. The more formal methods for rating the reputation of a site or of a user are also common. The eBay rating system tries to use customers' positive and negative feedback ratings as a measure of a seller's reputation [4]. Epinions, a consumer review web site, also allows customers to rate the transactions with sellers, and maintains a more explicit trust rating system [5]. The PageRank algorithm [Ridings and Shishigin, 2002] used by the Google search engine, is also a trust metric of a sort. It uses the number of links coming into a particular page as votes for that site.

Trust plays a major role in privacy-enhanced identity management (PIM), because users need to: "(a) trust their own platform to manage their data accordingly, and (b) trust the remote set of platforms that receive the identity data to deal with these data appropriately" [Andersson et al., 2005]. If the evidence is provided to the users that the data they disclose will be treated as defined, then this can potentially enhance trust of users in a data processing environment of the service providers.

The three most common types of trust solutions found in the literature are as follows: (a) based on digital certificates, (b) based on one's own past experience, and (c) based on the recommendations from peers. In digital certificate based trust, trust is binary one party is authenticated to be trustworthy or not. On the other hand, trust built by experience or recommendation is of a "softer" nature for example, the trust a user may have on a service provider could be defined as a value between 0 and 1.

[4] www.ebay.com
[5] www.epinions.com

In the literature, trust is identified in different forms relating to: whether access is being provided to the trustor's resources, the trustee is providing a service, trust concerns authentication, or trust is being delegated [Grandison and Sloman, 2000]. Abrams implicitly maps trust decisions to access control decisions
[Abrams and Joyce, 1995]. Generally, resource access trust should form the basis for specifying an authorization policy, which then is implemented using the operating system or database access-control mechanisms, firewall rules etc. A trust relationship can be refined into the authorization policies that specify actions the trustee can perform on the trustor's resources and constraints that apply, such as time periods for when access is permitted. For example, Fred is trusted to do Linux installations on Bob's machine. In e-commerce and e-banking, customers trust the vendor or the bank to support mechanisms that will ensure that their passwords are not divulged and prevent their transactions from being monitored. The vendor or bank is also trusted to maintain the privacy of any information, such as name, address, and credit card details, which it holds about the customer.

A trustor trusts a trustee to make decisions on its behalf, with respect to a resource or service that the trustor owns or controls. In other words, for a service X, A trusts B to make decisions on A's behalf about the resources that A owns or controls [Dimitrakos, 2002]. An example is the delegation of decisions regarding investment to one's financial advisor. Infrastructure trust refers to the base infrastructure that a trustor must trust [Gerck, 1998]. The trustor must trust him/herself (implicit trust). One should be able to trust their workstation, local network and local servers, which may implement security or other services in order to protect their infrastructure. An example of infrastructure trust is the PC's application software trusts the operating system.

Professional certification is a common technique used to convey a sense of competency trust in the medical, commerce, and engineering domains; and so could be applied to internet services. Certificates are commonly used to authenticate identity or membership of a group in Internet applications [Gerck, 1998]. Based on the notion that "certificates represent a trusted party," in certificate-based trust, a trustee

presents a set of certificates of trustworthiness to a trustor. For example, I may trust someone with a PGP certificate signed by two people I already trust. A certification authority (CA) issues a Digital Certificate to identify whether or not a public key truly belongs to the claimed owner [El-Khatib et al., 2003]. This is necessary to establish a resource access or service-provision trust relationship and may implicitly reduce the trustor's risk in dealing with the trustee. The limitation of certificate-based trust is that a CA does not vouch for the trustworthiness of the key owner, but simply authenticates the owner's identity.

PGP and X.509 are two of the main certificate systems in use (and trusted) to authenticate one party to another. Pretty Good Privacy (PGP) provides a way to digitally sign and encrypt information without the overhead (e.g. Computationally intense process, scalability issue) of a public key infrastructure. Unlike X.509 certificates, which come from a professional CA (a trusted third party) , PGP implements a mechanism called "Web of Trust", wherein multiple key-holders sign each certificate attesting the validity of the certificate [El-Khatib et al., 2003]. Phil Zimmermann first put the web of trust concept forth in the manual for PGP version 2.0: "As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys" [Zimmermann, 1994]. There are still, however, many uncertainties and risks that challenge certificate-based mechanisms [Ellison and Schneier, 2000]. For example, why and how can we trust a public key infrastructure vendor?

Trust Management Systems (TMS) have the goal of providing standard, general purpose mechanisms for managing trust. Blaze et al. define trust management as "a unified approach to specifying and interpreting security policies, credentials, and relationships which allow direct authorization of security-critical actions" [Blaze et al., 1996]. Examples of trust management systems include REF-

EREE [Chu, Y., 1997] and KeyNote [Blaze et al., 2003]. Some TMS make use of a trust policy language to allow the trustor to specify the criteria for a trustee to be considered trustworthy. REFEREE is a trust management system for making the access decisions relating to Web documents by evaluating requests and returning a tri-value and a statement list, which is the justification for the answer. A tri-value is either true, or false, or unknown. True means, "Yes, the action may be taken because sufficient credentials exist for the action to be approved", false means, "No, the action must not be taken because sufficient credentials exist to deny the action," and unknown means, "the trust management system was unable to find sufficient credentials either to approve or deny the requested action." Using the REFEREE policy language, a user can define the policy under which a web client decides when to fetch the credentials and how to evaluate them.

2.4 Personalization

The personalization consortium characterizes online personalization as "the use of technology and customer information to tailor electronic commerce interactions between a business and each individual customer" [Personalization Consortium, 2005]. Neuhold views personalization as the adoption and arrangement of services and information in coherence to a single user or a group of users [Neuhold, 2003]. In other words, it means permanently optimizing the presented information to the user's needs. As quoted in page 3 of Brown, 2001, Pattie Maes, the architect of one of the early personalization systems -Firefly, describes a personalized system like this [Brown, 2001]: "For me, an ideal system is really one which gives me a mix of things that I like, that are related to my past interests, but that also introduces me to new things and tries to push the boundaries of my taste. These kinds of systems can do this, because they have a model of what a user is interested in and they can give you stuff that is just outside your boundaries. There is an element of serendipity; not just tracking the changing interests of the user, but changing the interests of the user by introducing them to new things." The need for personalization arises from

a resistance to the "one size fits all" paradigm. For example, a resource developed for one device, such as a PDA, mobile phone, tabletPC, laptop or desktop, may not be suitable for another type of device. The preferences set for one user's interaction with a software application may not be appropriate for another user. Businesses are investing considerable resources in developing and deploying personalization systems for customer interactions. Yang and Padmanabhan produce several examples of successful personalization engines in use today [Yang and Padmanabhan, 2005]. Personalized systems help to decide which of the Amazon's or Oracle's customers were more likely to be trustworthy, more likely to spend money, or more deserving of better treatment. AT&T WorldNet uses a method to decipher the visitors' preferences unintrusively, and continually making suggestions to visitors based on learned preferences. DoubleClick uses visitor profiles to target banner advertisements on their clients sites that are more likely to be of interest to a specific visitor. Dell Computer provides personalized Web pages for its corporate customers that simplify placing and tracking orders.

A business can offer personalization in two ways: responding to individual specific characteristics and responding to collective knowledge of their entire customer base [Chellappa and Sin, 2005]. A store can offer personalization based on individual specific characteristics like name, shipping address and preferred mode of delivery, and preferences on volume discounts, etc. The companies on the Web can personalize purchase experiences of the customers. For example, Amazon and Barnes & Noble leverage the collective knowledge of their entire customer base to anticipate the preferences of each individual customer to make personalized recommendations. Using collaborative filtering technology (i.e., making automatic predictions about the interests of a user by collecting taste information from many users, the store can propose new music or book selections to the particular customers based on recommendations by other users who exhibit similar preferences.

Personalized systems are sometimes referred to as user adaptive systems, since an interaction is adapted based on data about an individual user. Adaptive systems are better able to cater to users' needs, the more data their user modeling system

collects and processes about them. Therefore, they collect as much data as possible and "lay them in stock" for future use [Kobsa and Schreck, 2003]. Personalization is critically dependent on the following two factors [Chellappa and Sin, 2005]: i) A vendor's ability to acquire and process consumer information, and ii) A consumer's willingness to share information and use personalization services. In the first type, information is gathered by the system implicitly observing and recording a user's behavior. In the second type, this can be done by explicitly asking a user about their interests or by deriving a profile of them from their browsing behavior. In return, the user can be supplied with information, which is really relevant for them.

Consumers are recognizing that they need personalization to help them manage the volume of information available to them. A 2006 survey [ChoiceStream Inc., 2006] conducted in the U.S. finds that 79 percent of the consumers are interested in receiving personalized contents, which is consistent with the response of 80 percent from the survey done in the year 2005. While interest in personalization remains high and consumers' willingness to divulge information increases, the concern about the security of personal data is consistent year over year, with 62 percent of consumers indicating concern in 2006 vs. 63 percent in 2005.

The net benefit of online personalization to consumers is the convenience gained from having different parts of the online browsing and purchase experience personalized. Broadly speaking, the online vendors construct consumer profiles based on various criteria, and they personalize products and services using different matching techniques for a particular consumer profile [Raghu et al., 2001]. The number of criteria describing a consumer profile varies with the context and technologies used for personalization. For example, Doubleclick uses 22 criteria in describing an anonymous consumer's Web browsing profile [Raghu et al., 2001].

Generally, a personalization system fits in one or more of the following categories: customizing access to information, filtering systems, recommender systems, tutoring systems, and search engines & systems [Neuhold, 2003]. An example of customizing access to information services is subscribing to the newsletter service of an internet newspaper where the readers can specify topics that are relevant for them (e.g.

politics & sports). Filtering systems, usually used for email messages or newsgroup postings, help users to get rid of unwanted materials (e.g. "Cybersitters" for preventing the children from accessing dangerous web sites). Recommender systems and services provide advice to users about the products or services in which they might be interested. Tutoring systems produce personalized learning courses that are tailored to various learning preferences and characteristics of the learners. All three major search engines offer personalized versions of their home pages: Google Homepage, My Yahoo!, and My MSN.

Since the objective of this chapter is to comprehend personalization to the extent it is necessary to relate its implications to privacy, the details of various personalization techniques are skipped. This section will end with a brief description of one specific popular personalization technology, collaborative filtering (CF) used by many Web sites and online service providers primarily because of its simplicity. There are two basic types of CF, user-based and item-based, both of which are pattern-matching techniques that base content 'recommendability' on correlations among user choices (e.g. purchases, downloads, ratings, etc.) [ChoiceStream Inc., 2004]. The user-based CF systems compare a target user's choices with those of other users to identify a group of 'similar-minded' people [Shardanand and Maes, 1995]. Once this group has been identified, a user-based CF selects the contents chosen, or highly rated, by a group of similar users to recommend to the target user. A user-based CF suggests that the consumers who choose A will prefer B and C, since other consumers in the database who chose A preferred B and C.

2.5 Relationship among Privacy, Trust, Security, and Personalization

Trust and privacy are inter-related constructs - the more we trust, the more information we are prepared to reveal about ourselves [Teltzrow and Kobsa, 2004, Briggs et al., 2004]. Since trust reduces the perceived risks involved in revealing private information, it is a precondition for self-disclosure [Steel, 1991]. Rezgui et al.

propose a reputation management system to monitor the reputation of web services and attribute high reputation to services that are not the source of any "leakage" of private information [Rezgui et al., 2003]. As a result, reputation-based trust can be used to manage privacy in web services. Chellappa and Sin also confirm through an empirical study that online consumers' concern for the privacy of their information is negatively correlated with the factors that build trust in the vendor offering personalization services [Chellappa and Sin, 2005]. People are not likely to reveal confidential information about themselves to an untrustworthy party. People even may be suspicious of data harvesting, if they feel that their personal information may be misused. Friedman et al. also suggests that trust in the online transactions is closely related to the issues of privacy [Friedman et al., 2000]. In the online world, trust invokes the threat of privacy violation, identity theft, and threat to personal reputation.

A person may choose to trade their privacy for a corresponding gain in another's trust. In an asymmetric trust relationship, one of the interacting partners is stronger. The weaker partner gets a higher level of trust by disclosing personal information. The weaker party must trade its privacy loss for a trust gain, which is required to start interaction with the stronger party [Lilien and Bhargava, 2006]. For a privacy-trust tradeoff, the users could be interested in answers to various privacy and trust related questions, such as [Lilien and Bhargava, 2006]:

- "How much privacy is lost by disclosing the given data?"
- "How much does a user benefit from a particular trust gain?"
- "How much privacy should a user be willing to sacrifice for a certain amount of trust gain?"

In face-to-face communication, one can look in the eyes of the interlocutor and search for tacit signs of truthfulness or falsehood [Feenberg, 1989]. On the other hand, the famous cartoon strip from the New Yorker could describe an online environment: "on the internet, nobody knows you are a dog." Privacy in the form

of anonymity could diminish trust. All the points below can contribute to an environment of diminished trust, which is not conducive to certain uses of computer communication [Johnson and Miller, 1998]: "(1) Anonymity makes law enforcement difficult (tracking down and catching on-line lawbreakers is difficult when their identity is unknown); (2) It frees individuals to behave in socially undesirable and harmful ways (individuals seem to engage in behavior they would not engage in if their identity were known); (3) It diminishes the integrity of information since one cannot be sure who information is coming from, whether it has been altered on the way, etc."

Briggs et al. state that trust has been identified as both a pre-requisite and a consequence of good personalization practice [Briggs et al., 2004]. In other words, an individual is more likely to disclose personal information in an atmosphere of trust, but the same individual is more likely to trust an organization that shows sensitivity to his or her personal circumstances. Chellapa and Sin's empirical study demonstrates that online consumers' intentions to use personalization services (and hence their willingness to share information) are positively correlated with the factors that build trust in the vendors' offering of the personalization services [Chellappa and Sin, 2005]. Trust promotes personalization and vice-versa. Users' trust can be expected to lead to more extensive and frank interactions, hence more and better data, thus better personalization [Kobsa and Schreck, 2003]. A good personalization practice may be a prerequisite for online trust building and vice-versa.

It is important to understand the difference between privacy and security. Security can both be an ally and an enemy to privacy. Privacy is generally approached as a social consideration, whereas security is seen as a technical concern. The relationship between them is that the security technologies might provide mechanisms by which privacy can be ensured [Dourish and Anderson, 2006]. Risks to privacy are among the various risks against which we might wish to be secure. Menard states that security is not the same as privacy, nor does an implementation of sound security practice guarantee that privacy will be achieved [Menard, 2006]. This is because privacy is most concerned with identifiable user data and users' rights to control what can be collected about them; what it can be used for; and to whom it may be

disclosed. The only way organizations can protect user data from misuse is by implementing policies, standards, and fair information practices [Cavoukian, 2006]. On the other hand, privacy cannot be obtained without security, since security provides the physical, logical, and procedural safeguards needed to keep information private.

Privacy can be realized through security by the means of access control and authentication. Information privacy relates to an individual's ability to control the use and the disclosure of information about themselves and determine who is permitted access to this information and who is not [Cavoukian, 2002]. While access control and authentication protections can safeguard against direct disclosures, they do not address the disclosures based on the inferences that can be drawn from the released data [Sweeney, 2002]. The use of authentication when it is not needed to achieve an appropriate level of security could threaten privacy [Kent and Millett, 2003]. Most individuals do not understand the privacy and security aspects of the authentication systems they are required to use in interactions with commercial and government organizations. As a result, individuals may behave in ways that compromise their own privacy and/or undermine the security of the authentication systems. As suggested by Demchak and Fenstermacher, the idea of the separation of knowledge about behavior and knowledge about identity could ease the tension between privacy and security [Demchak and Fenstermacher, 2004].

The secondary use of authentication systems (and the identifiers and/or identities associated with them) is related to linkage. Many systems are used in ways that were not originally intended by the system designers. The obvious example is the driver's license, whose primary function is to certify that the holder is authorized to operate a motor vehicle. However, individuals are now asked to present their driver's license as proof of age, proof of address, and proof of name in various circumstances. As discussed in "IDs–Not That Easy", the primary use of an authentication system may require security and privacy considerations very different from those appropriate for the subsequent secondary uses [Kent and Millett, 2002]. For example, a driver's license that certifies one is capable of driving a motor vehicle is quite different from certification that one is not a threat to airline travel. Given the difficulty of knowing

all the ways in which a system might be used, care must be taken to prevent secondary use of the system as such the use can easily lead to privacy and security risks.

Andersson et al. hint that a privacy and security solution can potentially lead to a trust solution [Andersson et al., 2005]. The secure and anonymous communication channels help establish basic trust in that they ensure that no data is leaked to the attackers, and the user releases no information regarding their network address and location. Access Control allows disclosure of data only if the other party has provided sufficient evidence of its trustworthiness and after an agreement on a data handling policy and obligation has been achieved. It enhances a user's trust in the protection of their personal data. On the other hand, recently, trust models have emerged as an important security risk management mechanism in P2P networks (e.g. in detection of malicious nodes [Kumar, 2006]).

Personalization can increase the potential for information processing, storage and retrieval. As Volokh observes, if we voluntarily turn over information about ourselves to facilitate personalization of our business arrangement, then the service providers will have even more information to record [Volokh, 2000]. Moreover, once recorded, this information can easily be communicated to others (usually for money). Since consumers need to provide preference information in order for the vendor to tailor its offerings to their tastes, personalization is infeasible to achieve without some loss of privacy. The win-win situation of users' gaining value and web vendors' making profit from personalization is impaired by privacy concerns [Kobsa, 2007]. Potential privacy concerns in personalized systems include ([Cranor, 2003]): unsolicited marketing, computer "figuring things out" about the user, fear of price discrimination, information being revealed to other users of the same computer, unauthorized access to accounts, subpoenas by courts, and government surveillance. The question, therefore, is if the online consumers will shy away from using personalization services. In this regard, prior research argues that people place a premium on their privacy [Culnan, 2000].

In summary, security can both enable (by safeguarding against unauthorized disclosure) and threaten (collecting and retaining personal information for authen-

tication) privacy. Privacy requires protection of identity information (i.e. personal information that contributes to identifiability of an individual), whereas security requires mostly monitoring of behavior information (i.e. activities that an individual pertakes). Identity information may only be required for identifying and sanctioning a bad actor only when bad actions are detected. A mechanism of separation of identity from behavior can allow monitoring of an individual's behavior without disclosure of their identity. Identity management may contribute to such separation of identity from behavior. In an identity management-based privacy solution, an entity ought to carry many partial identities, each is represented by a pseudonym. Activities (behaviors) of an entity can be attributed to a pseudonym. Partial identities should not be linkable, otherwise it defeats the purpose of limiting disclosure to a minimal amount of information. For example, the same email address of *BobTheBuilder* and *BobTheStudent* may allow one to link both partial identities, one representing Bob's avocation and other representing Bob's occupation.

2.6 Privacy, Personalization, Security, and Trust in E-learning

The realm of e-learning has been expanded from academia, to industry, to cyber communities. Today's web has experienced a momentous change from being the socalled Read-Web to a Read-Write-Web, which is based on participation and personalization. In consequence, e-learning has become a personal learning center where content is reused and remixed to cater to the students own needs and interests [Downes, 2005]. Besides institutional or corporate learning, informal learning widely takes place in personal networks, or in communities of practice, where members of a learning community both support and compete with one another, leading to effective and relevant knowledge construction.

Personalization of learning involves the presentation of a learning experience that is customized to the preferences of the learner [Dagger et al., 2003]. Borcea et al. see personalization as a need in e-learning, because of diverse learning objects, dif-

ferent cognitive abilities, different level of prerequisites, and different learning styles [Borcea et al., 2005]. Personalization of learning can involve the tailoring of tools, devices, communications, contents, etc. to the needs of the individuals. Personalization of learning is potentially beneficial in terms of time, money, and effectiveness. Dagger et al. suggest that personalization can be based on multiple paradigms [Dagger et al., 2003]. Context personalization is adapting to the preferences of the learner and semantics of the learner's current environment. Competency personalization is adapting to the learner's prior knowledge of the information domain being presented. Prerequisite personalization is adapting to the currently required prerequisites of the learner, such as a pre-session defines learning objectives and learning goals.

The notion of learner modeling, which is a prerequisite for personalization, is a process of capturing information about learners in relation to the learner's understanding of a domain. It can also refer to a global description of a learner's cognitive attributes to be used by an Intelligent Tutoring System to judge a learner's understanding of deep domain knowledge [McCalla et al., 2000]. The most common characteristics of a learner that can be modeled include a learner's goals, plans, capabilities, attitudes, affect and social aspects. McCalla suggests that learner modeling approaches will involve two activities: understanding the basic world view of the learner, essentially tracking information about an individual learner including his/her community memberships, and his/her relationships to others in the community, and the second activity involves tracking particular information about a learner which is important to the current system application [McCalla, 2000]. As in traditional face-to-face education, trust is an important concern in e-learning systems [Xu and Korba, 2002]. In the context of networking and distributed applications like e-learning, one system needs to be trusted to access another underlying system or service. Trusted interaction forms the underlying requirement of service between a user and the providers [El-Khatib et al., 2003]. For example, a service provider must trust that a learner truly has the credentials that are not forged and is authorized to attend the course, or is limited to accessing only some services. On the other hand,

the learner must trust the services. More importantly, the learner must believe that the service provider will only use his/her private information, such as name, address, credit card details, preferences, and learning behaviors in a manner expressed in the policy provided for the e-learning system users.

The trust levels of learners may also indicate their levels of motivation or aspiration for learning. An Internet-based e-learning environment that provides mutual trust, respect, and freedom becomes a happy and safe harbor for learning and teaching activities [Xu and Korba, 2002]. With the maturation of e-learning, trust becomes the most crucial factor for the success of a distance learning process. E-learning systems are different from many other online communities in that the learners typically have more trust in the system (i.e., are willing to share private information readily, especially if used for evaluation), and have long working relationship with one system (e.g. they may work with the same online discussion forum system for many years as they progress through school).

Collaboration is an important part of learning, whether it is in classroom settings or in virtual settings. Mason and Lefrere state that, in e-learning, common goals and mutual benefits are discerned and pursued through collaboration [Mason and Lefrere, 2003]. Collaboration minimizes the duplication of efforts and stimulates innovation. Allan and Lawless point out that online collaboration can cause stress, and this stress is linked to the dependency of the collaborators on one another, and the level of their mutual trust [Allan and Lawless, 2003]. An effective collaboration, whether synchronous (e.g. chat, conferencing) or asynchronous (email, blogs, threaded discussions), depends upon trust. Privacy awareness becomes even more important in a collaborative environment. The primary concern regarding privacy in collaborative work settings is "impression management" [Patil and Kobsa, 2003]. Since, in a collaborative environment, users interact with different users or user groups, various types of information about them accrue in the course of time [Franz et al., 2006]. A detailed user profile could be created by linking all the different actions of users as well as information disclosed during performing these actions.

Most e-learning innovations have focused on course development and delivery, with little or no consideration to privacy and security as required elements. E-learners are becoming perceptive about the privacy implications of their online activities, and different governments have recently introduced privacy legislation. Privacy provision and data protection are the basic requirements for corporate e-learning, especially, when the personalized systems that adapt to the sensitive learner's personal data are used. Besides, companies do not want competitors to learn the details of the training provided, which could compromise their strategic directions. In e-learning, privacy can be described as a learner's ability to control the conditions under which their personal information is shared with others [El-Khatib et al., 2003].

Borcea et al. point out that privacy requirements are obviously important for e-learning, since they establish an unbiased environment [Borcea et al., 2005]. A learner should be able to act under different partial identities or anonymously. The separation of activities encourages learners to be unrestricted and allow them to learn without pressure. Besides this separation, we need explicit linking of information by the owner of information so that they can build up reputation. For receiving unbiased evaluation, tutors and authors may only be recognized in one class. At the same time, an important goal of e-learning is to assist each individual user during the learning process. The prerequisite for an adequate assistance is to collect and evaluate information about a particular learner. Since an e-learning application aims at assisting learners, they cannot act in full anonymity [Borcea et al., 2005].

Xu and Korba identify the following security- and privacy-related concerns for e-learning services [Xu and Korba, 2002]: (1) Security: the concerns may include authentication, confidentiality, authorization, non-repudiation, etc. For example, users can access only those resources and services that they are entitled to access, and qualified users are not denied access to services that they legitimately expect to receive. (2) Privacy: mostly, this refers to the privacy of individuals. This includes all the individuals' concerns regarding the collection and the use of personal information. Borcea et al. and Franz et al. underscore two aspects of personal data that pertain to privacy protection of learners [Borcea et al., 2005, Franz et al., 2006]: (a) Data

Table 2.1: Users act within diverse roles [Borcea et al., 2005]

Role	Tasks/Interests
Technical Administrator	Administrates and manages the technical environment, manages policies, and grant initial permissions.
Content Manager	Provides and manages the overall structure of the e-learning environments, plans new classes, and commissions tutors and authors.
Author	Creates informative materials and test materials.
Tutor	Organizes classes, controls learning paths, gives assistances.
Learner	Gains knowledge, practices and asks, tests his/her knowledge.
Moderator	Moderates discussions in synchronous learning.
Anonymous user	Browses, i.e., informs himself about classes and groups provided by the e-learning environment, but cannot access learning content.

parsimony– store as little personal data as possible, and (b) Data partitioning - partition data into context-specific partial identities.

The European Future of Identity in the Information Society (FIDIS) project, investigating identity management, views privacy enhancing identity management as a natural solution to privacy management online [Jaquet-Chiffelle et al., 2006]. Privacy-enhancing identity management (PIM) enables users to act as they are used to in everyday life [Borcea et al., 2005]: they do not offer all information about them in each situation. Depending on the context, users decide which information is disclosed. In that way, learners should be able to separate acting within the e-learning environment from other roles in their life. Such a subset of information is called a partial identity (see potential partial identities in e-learning in Table 2.1). All the partial identities represent the user. The partitioned information, i.e., the data fragments, should not be linkable to the users' real identity. Only users themselves are able to explicitly link different partial identities. For example, this can be desired if they want to build up their own reputation.

Despite the need for unlinkability of different partial identities, we need a reasonable access control mechanism in order to prevent unauthorized accesses to material, annotations, or evaluation results. Therefore, the use of anonymous cre-

dentials [Camenisch and Lysyanskaya, 2001] for providing evidence of permissions is a reasonable choice. In an anonymous credential system (e.g. idemix by IBM [Camenisch and Herreweghen, 2002]), an organization can issue a credential to a pseudonym, and the corresponding user can prove possession of this credential to another organization (who knows the user by a different pseudonym), without revealing anything more than the fact that the user owns such a credential. Anonymous credentials enable users to unlinkably demonstrate the possessions of certain attributes.

The Privacy-enhanced Identity Management (PIM) platform provides the necessary functionality such as managing pseudonyms and credentials, and establishing anonymous communication. Furthermore, an e-learning application must be able to recognize context switches. The users must be informed if starting an action implies a context switch, and they must have the possibility to switch their partial identities in this case. The PIM client also supports the configuration of pseudonyms. Configurations may determine which data may be transferred if the user acts under this pseudonym, which credentials may be delivered if requested, and which action or set of actions imply a context switch. It must be transparent for the users which information others know about them. The actions that require permissions imply a negotiation phase. The credential system (considered as part of the PIM) at the server side issues credentials, which are delivered to the clients. The credential system of a PIM client component stores the credentials. It may select a subset of the assertions contained in a credential where the subset is agreed upon in the negotiation phase.

A privacy-aware e-learning environment can increase awareness of privacy threats as well as understanding of privacy-enhancing mechanisms, since e-learning is intended to transfer knowledge. For example, spyware, known to aid phishing, has been partly responsible for this fraudulent activity and the Webroot survey reveals that 48 percent of the teens and young adults have no understanding of phishing [6].

[6]Social Networking sites: A significant threat to online security, says report (source: http://www.publictechnology.net/)

Phishing attacks are aggressively disseminated through the social networking sites and activities favored by children and young adults. Since this environment has the character of a situation where learning and applying new concepts in order to gain experiences is usual, it can encourage users to really make use of the PIM concepts. Certified assertions by trusted third parties (e.g. TRUSTe) that confirm that the client software fulfills its specifications can be used to increase the trustworthiness of the client software for the users. If we were to create successful e-learning environments, we would have to include means and mechanisms through which we can foster online social interactions that can enable learners to form strong relationships [Nichani, 2000].

The social networking sites (SNS) are another frontier for exploring learners' privacy. Facebook is a social network that initially catered to College and High School communities. Facebook is of interest to researchers in two respects: (1) as 90 million registered [7] users represents an important phenomenon in itself: the behaviour of its users, the gains as well as the risks they face, and (2) as a quite unique experiment in information revelation, a source of highly valuable information about privacy attitude and privacy behavior among young individuals [Acquisti and Gross, 2006]. Previously, the privacy settings of Facebook were so permeable, and an external access (e.g., by non-students/faculty/staff/alumni, or by non-college-affiliated individuals, and so on) to the network was so easy that the network was effectively an open site [Gross and Acquisti, 2005].

After a rapid response to privacy backlash, Facebook has made changes to its current version to make it privacy-friendly including giving users the ability to control the publicity of an event or group on the community portal pages, enhancing privacy settings, allowing older and non-student users to join Facebook networks, etc. Since there is no mechanism available for users of Facebook to adequately understand contexts or assess the trustworthiness of another user, a user's apparent friend could be their worst enemy. According to its privacy policy, Facebook itself poses a threat to its users' privacy (in the form of link-ability): "Facebook may also

[7] http://www.pcworld.com/article/150489/

collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience." [8] Therefore, just allowing users to choose to disclose their personal information without enabling them to make a well-informed choice is not true control over disclosure that could contribute to preserving users' privacy. Moreover, recent events of Facebook's source code leak or displaying one user's personal information to other users due to proxy error suggest that users also need control over the usage of their personal information even after disclosure.

Category-based representations of a person's broad interests are a recurrent feature across most social networking sites [Maes, 2005]. Such categories may include the indications of a person's literary or entertainment interests, as well as political and sexual ones. In addition, personally identified or identifiable data (as well as contact information) are often provided, together with the intimate portraits of a person's social or inner life. Online social networking thus can morph into online classified in one direction and blogging in another [Gross and Acquisti, 2005]. The type of information revealed or elicited often orbits around hobbies and interests, but can expand from there in different directions. These include: semi-public information such as current and previous schools and employers (as in Friendster [9]; private information such as drinking and drug habits and sexual preferences and orientation (as in Nerve Personals [10]); and open-ended entries (as in LiveJournal [11]).

Observing online social networks, Danah Boyd notes, "there is no way to determine what metric was used or what the role or weight of the relationship is" [Boyd, 2004]. While some people are willing to indicate anyone as friends, and others stick to a conservative definition, most users tend to list anyone who they know and do not actively dislike. This often means that people are indicated as friends even though the user does not particularly know or trust the person. As a result, the

[8] http://www.facebook.com/
[9] http://www.friendster.com)
[10] http://www.nerve.com/login/LaunchPad.asp
[11] http://www.livejournal.com/

ability to meaningfully interact with others is mildly augmented, while the ability of others to access the person is significantly enlarged (in 2007, researchers found that two in five Facebook users happily divulged details such as their date of birth, phone number and workplace to people whom they have never met [12]).

Gross and Acquisti identify the following reasons for the unchallenged acceptance of the permeable default privacy settings of a social networking site [Gross and Acquisti, 2005]. Peer pressure and herding behaviors and relaxed attitudes towards (or lack of interest in) personal privacy are the top two reasons. The other reasons include incomplete information about the possible privacy implications of information revelation, faith in the networking services or trust in its members, and myopic evaluation of privacy risks or also the service's own user interface. Moreover, the college-oriented networks offer a wealth of personal data of potentially great value to the external observers because of these aforementioned reasons. For example, the New York Times reports that the Pentagon manages a database of 16-to-25-year-old US youth data, containing around 30 million records, and continuously merged with other data collected for focused marketing [Cave, 2005]. Broadly speaking, all the privacy solutions for e-learning found in the reviewed literature can be grouped into four categories:

- Identity Management
  - Disclosure decision
  - Identity provision
  - Identity protection
  - Identity presentation
- Privacy friendly access control
  - Credentials
  - Policies

[12] http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2253720.ece

  - Trust management

- Anonymous communication (mix networks, onion routing, etc.), and

- Education & awareness

2.7 Conclusion

In the process of comprehensive reviewing of the privacy related literature, a few interesting open issues are identified, which in turn motivate the research presented in this thesis:

- The need for information sharing is as important as the need for privacy. Privacy is not about avoiding disclosure, but rather, context-dependent selective disclosure. Therefore, a privacy-enhanced information sharing paradigm is highly desirable yet not easily provided.

- The existing notions of privacy are predominantly concerned with disclosure of personal information. However, the usage and retention of an individual's information beyond their anticipation may pose greater risks to privacy.

- To treat the issues of privacy squarely, the related issues (other variables that positively or negatively influence privacy) like security, trust, personalization need to be considered.

- Secondary use of authentication systems (and the identifiers and/or identities associated with them) is related to linkage. There is a need for mechanisms to restrict secondary use. An appropriate authentication system must follow the data parsimony principle. For example, a graduate student holds multiple partial identities based on the role they play: a student, a tutor, an instructor or a marker. In the context of being in a teaching role, one's student id number may be extraneous information whereas in the context of enrolling in a class, employee id may be irrelevant.

- Information expiration minimizes the risk to privacy loss (as Holtzman describes it as the sin of latency [Holtzman, 2006]). Information expiration allows its owner to have adequate control over their disclosed information. Developing a model to enforce the mandatory forgetting of information seems to be very difficult yet a quite significant step towards privacy preservation.

- The trustworthiness of an entity is typically measured with the knowledge about the entity (or his/her multiple identities), which raises concerns over privacy. A mechanism to attach and remove reputation with a pseudonymous identity could help facilitate trust without the loss of privacy. For example, as learners interact with one another, familiar pseudonyms emerge and attribution of personalities to pseudonyms quickly develops. An e-learning system should help users identify potentially good collaborators or helpers, they can work to build a relationship of trust.

- Since users assume many pseudonyms to represent many aspects of their identities, there is a need for reputation transfer among the pseudonyms without letting anyone link one pseudonym with the other. In an e-learning community, actors sometimes assume numerous pseudo-identities (e.g. student, tutor, instructor) to allow them to explore different aspects of their persona, interests or hobbies. However, by switching to another pseudonym, the learner cannot use the reputation, which their current pseudonym has earned over a period.

- The context of use of personal information is an important factor in making users comfortable with sharing personal attributes. The context could be formalized using purpose-based models of learning interactions, where a specific learning purpose (e.g. to evaluate a student vs. to provide help to a student) is mapped directly to attributes required to support it (e.g. student marks, learning style, or online activity). Integrating this into an e-learning environment in an unobtrusive yet customizable manner is an important goal of a privacy-enhanced learning environment.

The above listed open issues have inspired me in setting up the research goal of designing a privacy-preserving information sharing paradigm. Since an individual's expectation of privacy is influenced by different factors, in order to design a privacy-preserving information sharing paradigm the research question important to be addressed first is the following: **What key factors need to be addressed to holistically support a privacy-preserving information sharing paradigm?** Since privacy is a subjective and fluid notion, a solution to privacy needs to integrate users in making the decision of disclosure. Moreover, such a solution needs to consider an individual's expectation of privacy together with their need for sharing personal information. Therefore, the second research questions is formulated as follows: **How could one construct a user-centric computational model for privacy which caters to various information sharing needs, especially as required for personalization in e-learning?**

Chapter 3

Privacy-preserving Information Sharing

This thesis investigates privacy-preserving information sharing in the online world based on context-sensitive identity construction and trust evaluation. The scope of this research includes constructing a generic model for privacy, verifying and validating the model against various privacy principles and central research questions (presented in Chapter 1). To facilitate privacy-preserving information sharing, the Identity and Trust based Model for Privacy (ITMP) supports trust-based selective disclosure of information, information expiration, and restriction on secondary use of information. To facilitate trust, this model incorporates a model for privacy-preserving reputation transfer (RT) across partial (contextual) identities. As a representative domain of the online world, e-learning has been used as a testbed for verifying and validating the constructed models.

The primary objective of this research is to achieve a possible user-centered solution to privacy concerns without restricting personalization. The motivation for this research underpins the following two observations: (a) Individuals have varying needs for privacy, and the amount of privacy one seeks today changes over time and (b) In many different contexts, both privacy and personalization are desirable and hard to trade one for the other. The ITMP model is constructed based on the following principles extrapolated from various research done to date on privacy and related issues: (a) privacy is context-dependent selective disclosure of identity, (b) privacy and trust hold a symbiotic relationship, and (c) the knowledge of identity disallows privacy, while the knowledge of behavior enables personalization. This thesis recognizes that privacy is not achievable without infrastructural security, and a comprehensive study on existing technologies for security (presented in Chapter 2)

suggests their effectiveness in providing security required for privacy. Therefore, the ITMP model assumes that infrastructural security required for privacy is available.

3.1 Privacy in an Information Sharing Paradigm

In general, privacy is viewed as users' control over their personal information. In the reviewed literature, much attention is given to protecting information before disclosure and making judicious choices about sharing information. However, many privacy infringements creep in due to insufficient user control over the once disclosed personal information. A privacy-preserving interaction paradigm is presented in Figure 3.1. A person may assume many contextual partial identities to represent them appropriately in many different contexts. Each partial identity may divulge personal information under various identifiers (pseudonyms). Information disclosed under one partial identity of an actor should not establish links to their other partial identities. For example, in an e-learning environment, a learner's one single identity encompassing all attributes can be fragmented into partial identities, two of which might be used to represent them in helping and help-seeking contexts. A partial identity in a help-seeking context may be represented through multiple pseudonyms, say, *JoeTheHelper* or *BobTheHelper*. The dotted rectangle in Figure 3.1 shows a boundary inside which, ideally, disclosed information should be retained. The overarching goal of the models (both the ITMP model and reputation transfer model within) presented in this chapter is to achieve privacy-preserving interaction between actors.

3.1.1 Definition of Privacy

Expanding on the widely perceived notion of privacy as control over personal information, I posit that information privacy boils down to control over three aspects of personal information: flow, boundary, and persistence (shown in Figure 3.2). For the purpose of this research, privacy will be defined as users' control over the flow, boundary, and persistence of their personal information. Flow is defined as the act of

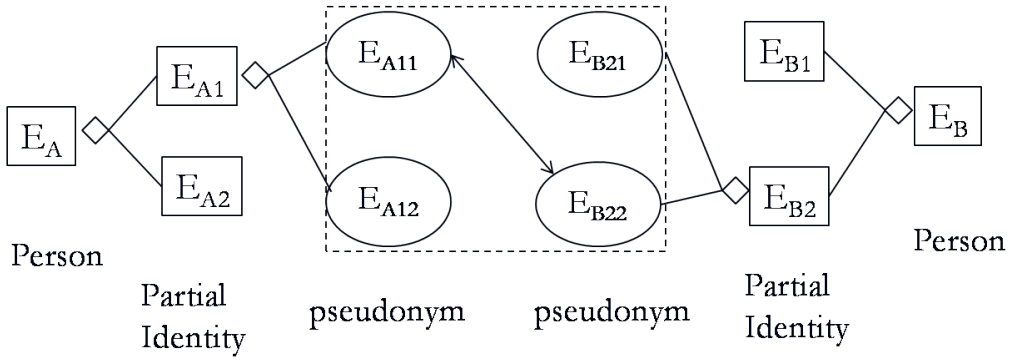


Figure 3.1: A privacy-preserving information sharing paradigm

sharing information with a partner. Boundary of information is defined as the scope or realm within which shared information to be used. Persistence of information is defined as the period of time shared information be available to or usable by a partner with whom information to be shared. The flow of disclosed information dictates which piece of information should flow from an information source to an information sink without leakage. The boundary of disclosed information dictates the perimeter or context within which information should be retained. When a piece of collected information is repurposed, the boundary of that piece of information is pushed. The persistence of disclosed information refers to the temporal aspect of that information. An archived and outdated piece of personal information of a person makes that person vulnerable to misrepresentation. For example, a Google search revealing a person's past political affiliation may not accurately represent them at the current time.

These three aspects are not entirely independent, but they are distinct. The boundary and persistence of information are of concerns for privacy only when the flow of information takes place. The boundary or persistence of information may trigger the flow of information. When the boundary of information is pushed, information may flow to a new space. When information persists, it may flow to a new space. The persistence of information may push the boundary of information. Also, as the boundary of information is pushed, information may persist longer in the new space. For example, recently, Senator Clinton's letters to a friend written when she was 19 were published in the New York Times. In this case, the boundary

of information is pushed when the letter is acquired by the New York Times. As a result of publishing this letter, the information in the letter may persist longer than otherwise. Based on the above mentioned three aspects of personal information, I propose a three dimensional notion of privacy for an information sharing paradigm to address users' control both regarding disclosure and the usage of their personal information after disclosure.

If information does not flow from an individual's personal space to someone else's space, that person is in full control over their information, and there is no reason to worry about privacy. As a result, flow of information initiates an expectation of privacy. When an individual shares a piece of information, that individual sets the parameters of flow according to their expectation of privacy. For example, we do not share our personal feelings with anybody, rather, we deliberate in choosing our confidant. We may choose some cryptographic protocol to restrict any leakage in the flow. To enjoy privacy, control over flow is necessary, but not sufficient. Once information is transported to someone else's space, we trade control over our information (privacy) for trust. Our anticipated privacy then depends on the boundary and persistence of the disclosed information. Without control over the boundary of disclosed information, a disclosed piece of information may propagate to unanticipated spaces or used for unanticipated purposes. Without control over the persistence of disclosed information, a disclosed piece of information may remain with others for long time posing risk to privacy. In the archivable and searchable online world, control over boundary and persistence is necessary for privacy. With control over flow, boundary, and persistence, an individual enjoys total control over their personal information, and thereby enjoys privacy. Therefore, an individual's control over flow, boundary, and persistence of their information is sufficient to ensure their intended level of privacy.

A decision about the flow of information should be made before disclosure, while the issues of control over boundary and persistence of previously-disclosed information are realized after disclosure. Privacy-preserving information sharing is only possible when information owners enjoy an intended degree of control over their dis-

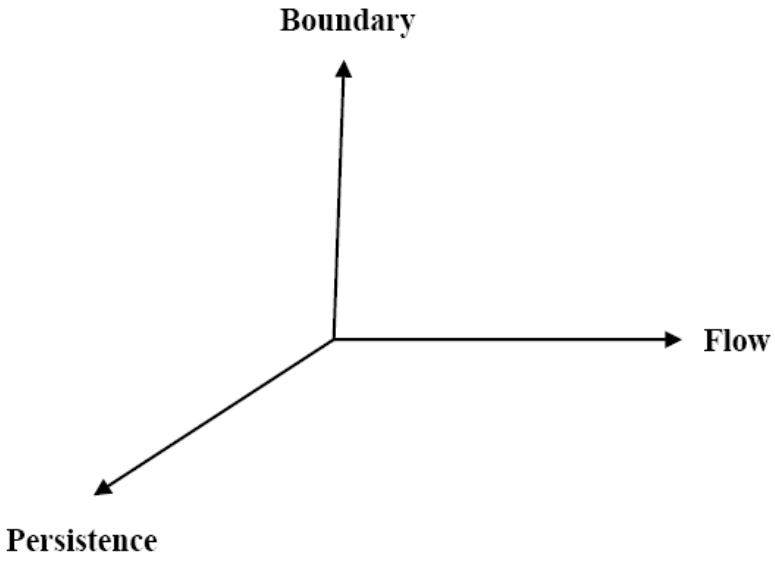


Figure 3.2: A 3-dimensional notion of privacy

closed information. I posit that if an information seeker is subjected to control over the flow, boundary, and persistence of personal information of an information owner, then the information owner can enjoy privacy while sharing personal information. As a result, an impostor will not have access to someone's personal information, and an information seeker will not be able to repurpose or retain information any longer than an information owner wants.

3.1.2 Preserving of Privacy

The intended control over the above mentioned three aspects of personal information can be achieved by the following three means: (a) selective disclosure, (b) restrictions on secondary use, and (c) expiration of information (shown in Figure 3.3). Selective disclosure allows an information giver to reveal their identity (thereby a set of personal information) according to their negotiated relationship with an information seeker. In the non-online world, we constantly evaluate our relationship with other actors and disclose our personal information selectively. For example, children are taught not to talk to strangers. Therefore, selective disclosure can ensure the appropriateness of the flow of information. Restriction on the secondary use

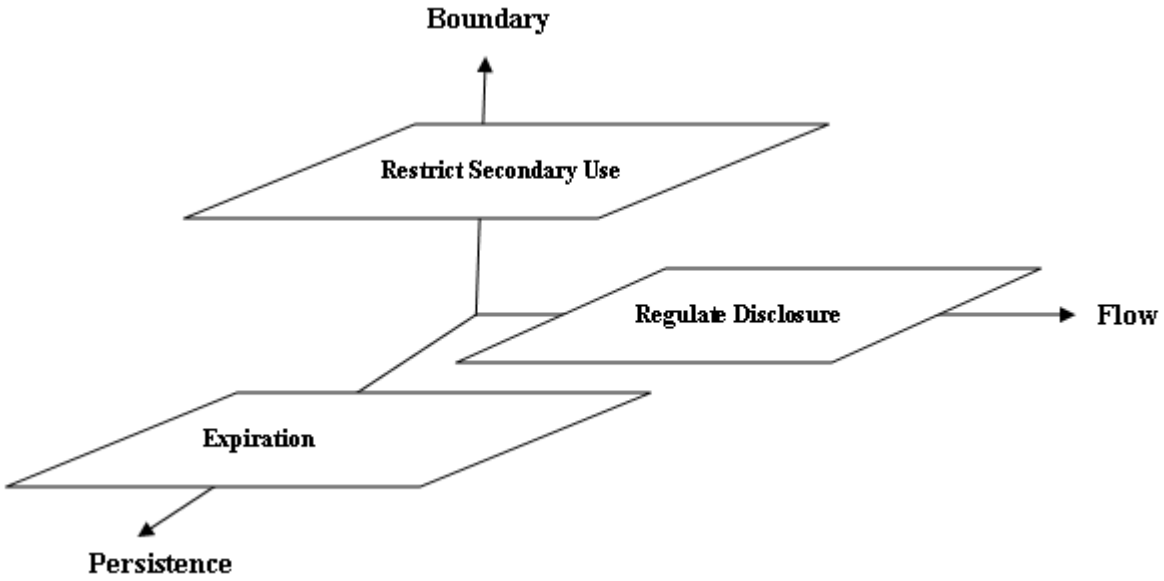


Figure 3.3: Approaches to address different dimensions of privacy

of personal information ensures that information is used in line with users' defined purposes. Due to secondary use of personal information, seemingly innocuous transactions can morph into privacy threats. For example, companies collect information for some purpose, and later on, sell that information to other companies. As a result, the boundary of information is pushed further than that of an information giver's anticipation.

In this context, expiring information means making information outdated through passage of time. For example, expiring a particular phone number information after a year of use will mean getting a new number after a year and no longer using that previously used phone number. Expiration of information restricts proliferation of an individual's personal information and protects the information owner against various privacy risks like misrepresentation, identity fraud etc. As long as a piece of information is available, it is susceptible to misuse. Since the online world lacks the quality of forgetfulness, the privacy threat in the online world is more serious than in the non-online world. Any information disclosed on the Internet is archiveable and searchable by a search engine. Expiration of information would allow the information giver to limit the duration of information persistence.

In addition to flow, selective disclosure may also contribute to controlling the boundary and persistence of information. For example, if an individual discloses information to a highly trustworthy counterpart, the counterpart is most likely to maintain that individual's desired boundary and persistence of information. Restriction on the secondary use of information may restrict an unanticipated flow of information. Information expiration may restrict the flow and boundary of information. If a piece of information is outdated and does not concern a person of interest, there is no reason to change the flow and boundary of that piece of information. Even though there are more subtle interactions of selective disclosure, restriction on secondary use, and expiration of information on boundary, flow, and persistence, the major impacts are on these axes (shown in Figure 3.3).

In summary, an individual's expectation of information privacy can be fulfilled by enabling them to control flow, boundary, and persistence of their information. Selective disclosure is about selectively sharing information, which involves making informed decisions about controlling the flow of information. Boundary control can be achieved through restricting secondary use of information. For example, the secondary use of a driver's license for identification when buying cigarettes pushes the boundary of information presented in a driver's license card. Persistence control can be achieved through expiring information. When information is no longer associable to a person, it expires.

3.2 Identity and Trust based Model for Privacy (ITMP)

In this section, I will present a model for privacy based on identity and trust. The ITMP model enables privacy-enhanced communications through understanding context, negotiating identity, and using trust. First off, this model constructs a partial identity for an individual by grouping context-relevant information under a transactional identifier or pseudonym, and then, in a well understood context, an individual may share the personal information associated with their partial identity with a

trustworthy information seeker. The model consists of five layers: application, context, trust, identity, and presentation (shown in Figure 3.4). Solid arrows indicate essential communication, and dotted arrows show if-need-be communication between entities (e.g. an information seeker and an information giver) at different layers.

Since (as stated in the previous sections) the three dimensions of privacy (i.e., control over flow, boundary, and persistence of shared information) can be reached through following three means: selective disclosure controls flow, restriction of secondary use controls boundary, and expiration of information controls persistence, the sub-goals of the ITMP model are to provide information-sharers with mechanisms to disclose information selectively, to restrict secondary use of disclosed information, and to regulate expiration of disclosed information. Based on the principle that privacy and trust hold a symbiotic relationship (which was drawn from the comprehensive review of literature presented in Chapter 2 and further substantiated by real world observation), the ITMP model uses trust to manage privacy. Trust is associated with the reputation of an individual. As a result, facilitation of reputation building in the form of reputation assessment and transfer across different partial identities emerges as another sub-goal of this model.

In Figure 3.4, the application layer provides the ability for users to initiate communication with the application layers of their counterparts. The tasks of this layer include identifying the counterparts, the purpose of communication, and the information being sought (in short, Purpose-Partner-Information or PPI). The context layer takes in information collected at the application layer regarding a partner and determines the context of a communication through identifying the role of a partner and assessing the relationship with the partner (in short, role-relationship or RR). Using the respective context information from the context layer, the trust layer assesses the trustworthiness of a purpose (e.g. integrity of purpose) and a partner (e.g. a partner delivering to privacy expectation) (in short, TPP). Based on the trustworthiness of the purpose and the partner, the identity layer constructs a contextual partial identity from a complete identity. The presentation layer ensures that an actor only discloses a set of information that is a subset of their respective contextual

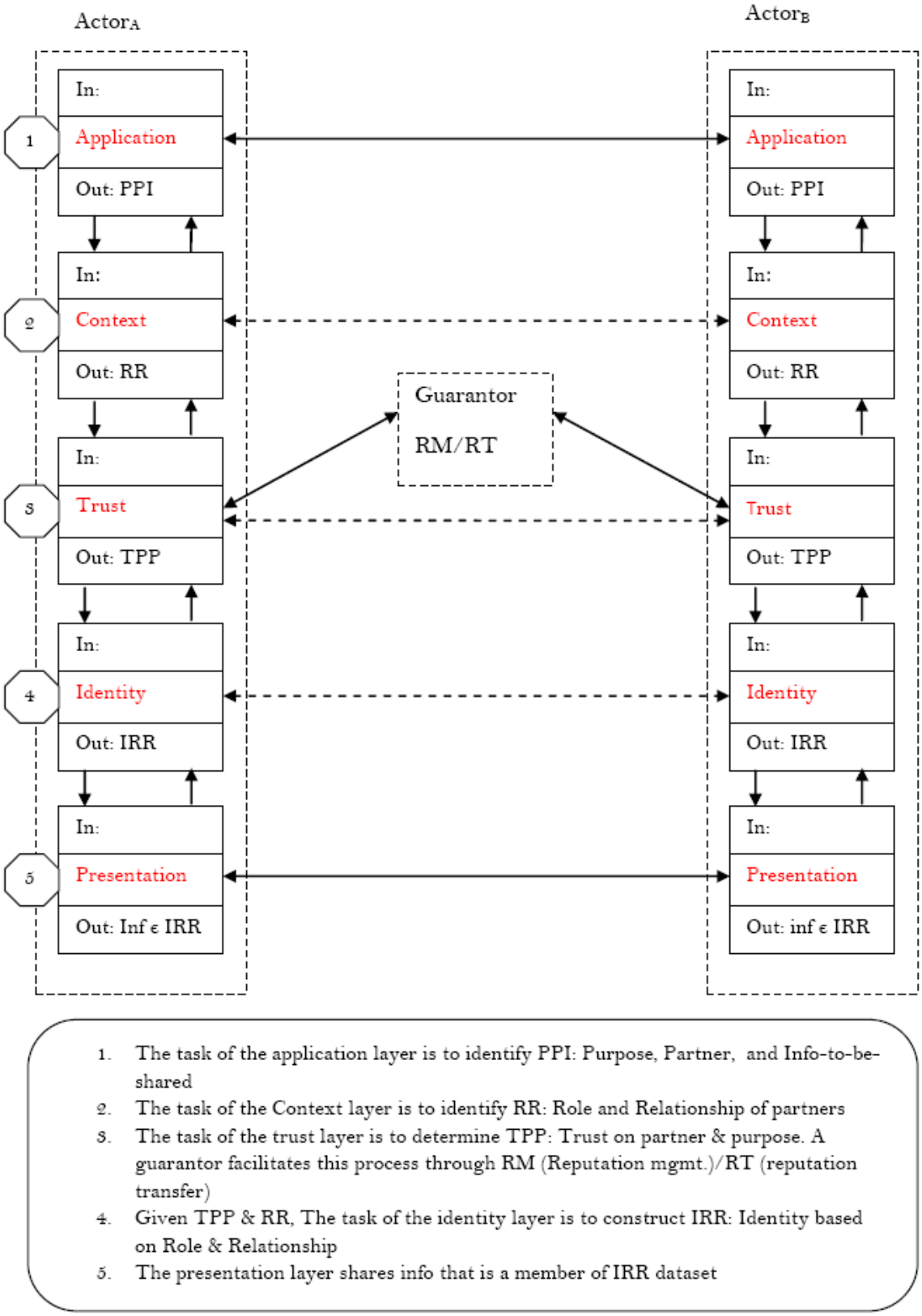


Figure 3.4: A 5-layer model for privacy

identity information.

The application layer performs the following three tasks:

(a) **Identify the counterparts:** In a communication episode, a person may maintain anonymity or present their pseudonymous or true identity. A person may claim an identity as their own by presenting credentials (e.g. userid/password, certificates) issued by a trusted introducer or a certification authority or claims (self-asserted credentials). The system facilitating the communication may identify its users through verification of credentials and may act as a trusted introducer of a user to another user. With the use of existing security technologies, such as digital signature, an individual can be more reliably associated with an identity without full disclosure.

(b) **Identify the purpose of communication:** Identifying the purpose of a communication episode may involve collecting several pieces of information from the communicating partners. A purpose could be stated at different level of granularity. To avoid ambiguity and establish a common understanding of purpose, a predefined machine-readable template should be established to express "purpose" using an XML-like language. The system providing the communication channel may force its users to choose from a list of allowed purposes in a communication episode.

(c) **Identify information being sought/ information to share:** In a communication episode, both the communicating partners need to decide on what information they need to know from each other. They also need to deliberate on what information they want to share with each other.

The context layer performs the following two tasks:

(a) **Identify the role of a partner:** Our world is full of roles. Learner, tutor, content manager, and instructor are some familiar roles in an e-learning environment. Every actor in a communication episode plays a certain role. Understanding a role is important to understand a communicating partner

correctly. A role can be defined as a set of expected behaviours attached to the position of an individual in a community. An online system may assign different roles to groups and individual users to build an online community. Roles of individuals may govern the flow of information between them. For example, individuals in learner roles may share marks with their advisor, but an advisor need not do the same. The system may identify an individual's role by authenticating their role-based certificates.

(b) **Identify the relationship:** A relationship is a specific connection manifested in individualized interaction between two roles. For example, in an advisor-advisee relationship, a teacher engages in personalized communication with a student for guiding the student in making academic choices. A relationship defines duties of involved roles (individuals) towards each other. A relationship can be formally presented in any policy specification language or XML-based markup language.

The trust layer performs the following two tasks:

(a) **Trustworthiness of a partner:** It helps decide whether the claimed identity of a partner may be trusted. It may also help decide whether the partner ought to be trusted with the information being sought. In the online context, trustworthiness of a person can effectively be measured through their reputation. Reputation can be assessed along the dimensions of competence, benevolence, and integrity. In a privacy-preserving information sharing context, a partner's competence to judge information correctly in a context is critical. Benevolence of a partner for not using one's information in a way that is disadvantageous for the owner is another form of trustworthiness related to privacy. Integrity of a partner may mean willingness to fulfill the conditions of usage of information stated by the owner of information.

(b) **Trustworthiness of a purpose:** An assessment of trustworthiness of a purpose is about deciding whether the information being sought is necessary or

relevant or irrelevant in a given purpose. It could be a subjective decision by an intelligent agent or person or may be expressed in a policy language.

The identity layer constructs a contextual partial identity of a person. With the understanding of context and trust, a person needs to decide on what identity to expose to another person. Constructing a contextual partial identity involves partitioning identity attributes and relevant reputation which are appropriate in a context to share with another person. Finally, the presentation layer discloses a piece of information that is a part of their contextual partial identity. It may also specify the conditions of usage (e.g. time-to-live and purpose-to-live tags) of that disclosed piece of information.

3.3 Context (Roles and Relationships) in ITMP

There is very little agreement on the definition of privacy. A primary source of this disagreement is the fact that the term "privacy" is used loosely by lay persons, scholars, and legal practitioners in different social contexts referring to different things [Yao et al., 2007]. Therefore, it is important to operationalize "context" for building a privacy protection tool.

In this model, roles and relationships are used to capture the notion of context to address privacy. A role encompasses a set of activities assigned to an actor or expected of an actor to perform. For example, an actor in a learner role is expected to be involved in various learning activities, such as attending lectures, participating in a course discussion, appearing in exams, etc. A relationship involves related entities of roles performing activities on one another. For example, in a learning-teaching relationship, both the learner and the teacher perform their respective roles. The individual variations in activities warranted by each role are affected by the perception of closeness of a relationship. In a closer relationship with a higher degree of trust, interaction may become less guarded. For example, two learners may interact with the same instructor differently based on the trust associated with their respective relationships with the instructor.

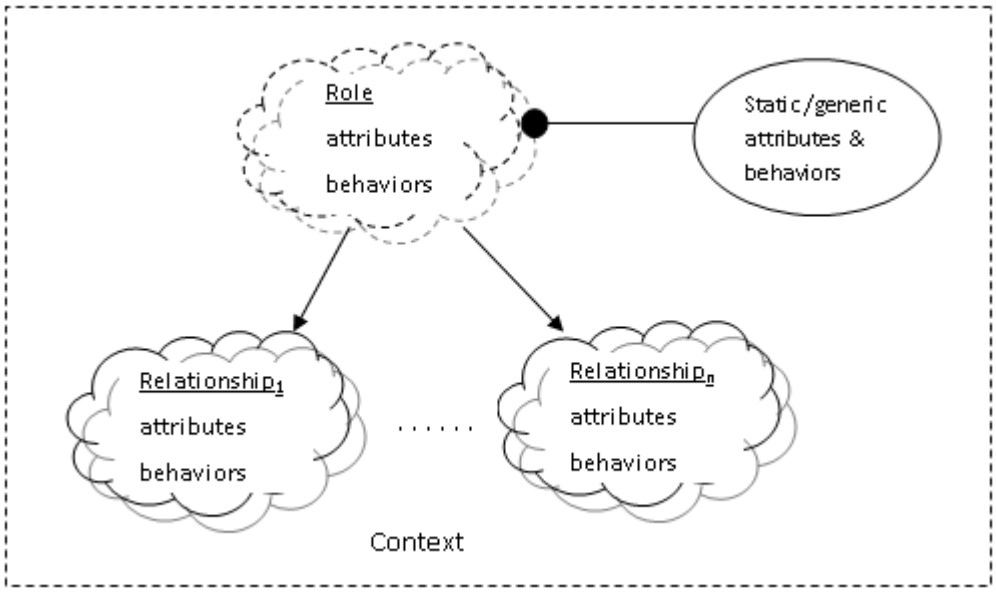


Figure 3.5: A role-relationship based notion of context

A role specifies duties or responsibilities (expected behaviors), and qualifications (attributes) of an actor (shown in Figure 3.5). In an information sharing paradigm, the roles of partners (e.g., information seeker and information giver) have to be well-defined and understood by one another. Attributes and behaviors possessed by a familiar role are mostly predictable and static. For example, students can easily predict the role (attributes and behaviour) of an instructor. But relationship is a dynamic concept, and therefore, it has to be measured against some subjective thresholds of partners in that relationship. In other words, a relationship between two actors can be measured as to what extent they meet each other's expectations (i.e. expectation of privacy, expectation of trust, etc.). As depicted in Figure 3.5, an actor in a specific role holds various degrees of relationships based on their different degrees of expectations on their communicating partners. For example, Bob in a student role may maintain different level of relationships with fellow students - some are more intimate, trustworthy, or private than others.

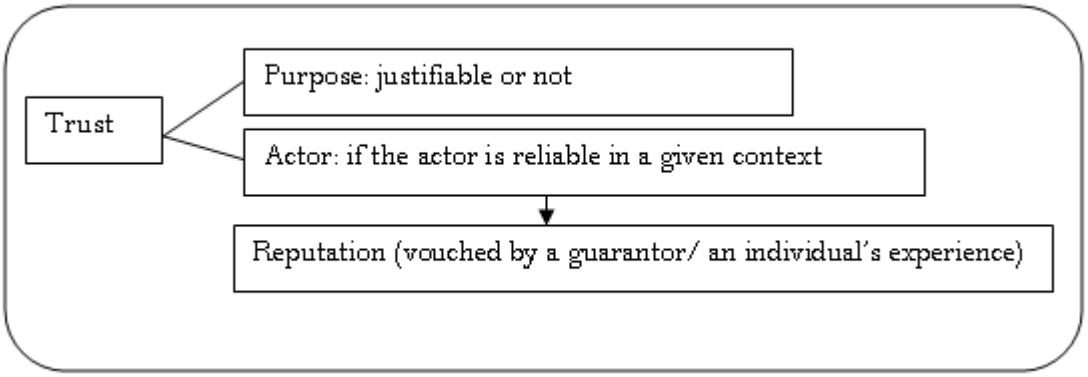


Figure 3.6: Use of trust in privacy-preserving communication

3.4 Trust in ITMP

In the ITMP model, trust is realized in two forms: trust in partners and trust on purposes (shown in Figure 3.6). The first form of trust assesses the trustworthiness of a partner in a given context. For example, a stranger is considered untrustworthy to be given a home phone number. The latter form of trust determines the relevance or justification of a purpose for seeking data in a given context. For example, seeking/providing a SIN number for the purpose of enrollment in a student organization is unnecessary. A known and tested trustee can understandably be retrusted or reevaluated based on the personal experience of a trustor. In the online world, however, a software manifestation of a trusted persistent public actor, namely a guarantor, is required to help find a trustee, because we interact with so many of actors, with most of whom we have no prior or persistent relationship.

This model assumes that the need for trust is contextual. For example, a high degree of trust is expected of somebody in a fiduciary role (doctor, lawyer, etc.). Trust is more prominent in a closely-knit community than in an open community. Trust is an important and deciding factor in a relationship. As trust grows in a relationship, flow of information increases between the related actors. As a result,

trust makes an information giver vulnerable to an information seeker. An information giver needs to know whether an information seeker is competent to understand the context of disclosed information. A trustee (trusted information seeker) acts in line with a trustor's expectation, and therefore, values an information giver's privacy choices regarding the flow, boundary, and persistence of their personal information. Above all, a trustee needs to be benevolent not to use a trustor's information in a manner that is disadvantageous to the trustor.

3.5 Identity in ITMP

Identity may be considered as a dataset (e.g. name, biometric data element, behavioral pattern, etc.) that is used to model and thereby recognize a person as distinct from others. A person may be represented by many identity models including their own "true" identity. Naturally, some models are partial, revealing some but not all information about the person. Some models may be incorrect - representing false information about the person. Sometimes, a person may want to publish their own personal identity models, and sometimes they may want to keep them concealed.

A partial identity is a subset of an identity set pertinent to a respective context. An individual holds multiple partial identities in different contexts. A partial identity should adequately represent an individual in a specific role in a specific context. Partitioning a person's one single identity encompassing all attributes into multiple partial identities contributes to the parsimony of information which, in turn, contributes to privacy. For example, a graduate student holds multiple partial identities based on the role they play: a student, a tutor, an instructor or a marker. In the context of being in a teaching role, one's student id number may be extraneous information whereas in the context of enrolling in a class, employee id may be irrelevant. In this model, once a context is understood and trust is established, a contextual partial identity map ("attribute-value pair") is constructed for potential disclosure.

Each partial identity (a contextual identity) can be presented with many different identifiers or pseudonyms. However, an actor in a specific role or a relationship

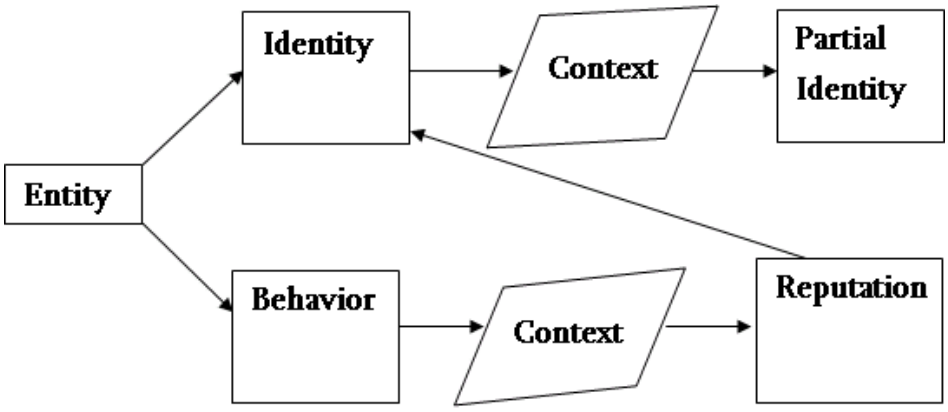


Figure 3.7: A contextual notion of identity and behavior

needs to be identified by the use of a persistent pseudonym. The person's dataset can be divided into two proper subsets: identity and behaviors. An identity (or partial identity) of a person needs to be comprised of personal attributes and reputation earned over behavior. However, behavior itself need not be a part of an identity, and therefore, identity and behavior are separable. This model argues that the longitudinal study of just the behavior part of a person could sufficiently assess reputation of the person in a given context (shown in Figure 3.7). Similarly, personalization can adequately be supported by aggregating an individual's behaviors over time in a given context over a persistent identity marker.

ITMP enables users to be selective in sharing information through analyzing context, assessing trustworthiness of communicating partners and justifying the purpose for which information is being sought. In this model, information expiration and restriction on secondary use are achieved through disassociating disclosed information from its owner's pseudonym. This can be achieved in the worst case by decommissioning the pseudonym. Privacy is at risk only when disclosed personal information and the owner (identity) of such information are associable. For that reason, an individual enjoys ultimate privacy as long as they are perceived as strangers (unidentifiable actors) by the observers. Even though a pseudonymous actor's behavior is observable, their true identity is unknown. In this model, a contextual partial identity is constructed for every context (role and relationship). And for every new information

request, the role of the information seeker and the relationship is reevaluated, and as a result, new identity may be reconstructed and the old identity may no longer being used. Therefore, identity is expirable, resulting in disclosed information becoming unusable. In effect, information expires and secondary use of information is restricted.

3.6 Example Scenario for ITMP

This section presents a scenario to further explain the ITMP model. Alice and Bob both have registered in an online offering of a course. In the course discussion board, Alice approaches Bob in search of a potential study partner. After introductory communication initiated at the application layer of the model at both users' ends, the purpose of communication, partner, and information sought are identified. In this case, the counterpart's pseudonym, the purpose extracted from discussion board message (i.e. seeking lab partner, and the information requested (e.g. an email from anybody who is also looking for a lab partner)) are gathered. The information gathered at the application layer is then fed to the context layer. The context layer helps understand the communicative context in terms of role and relationship of communicating partners (i.e. Bob and Alice). In this case, using their pseudonym, the counterpart's (e.g. Bob's or Alice's) role as a registrant of the same course is identified. Furthermore, one's perceived level of relationship with the other may be traced from their past interaction.

For a well defined context, the trust layer measures the trustworthiness of the partner (Alice or Bob) and justifiability of the purpose for which one partner seeks information from another. In this instance, one's reputation in the context of learning is measured, and justifiability of email for the purpose of seeking a lab partner is determined. The identity layer constructs a partial identity for a potential information giver based on their counterpart's role, perceived level of relationship with their counterpart, and expectation of trust from their counterpart. If the communicative context (role and relationship) for Alice and Bob is well understood and they appear

to be trustworthy to each other in the given context, a set of context-appropriate information is grouped under an identifier. This is called "construction of an identity". For their newly constructed identities, Alice and Bob are advised to pick a new pseudonym. Suppose Alice and Bob pick A and B respectively.

During the course of lab-partnership, A or B may share any information that is pertinent to their newly constructed contextual partial identities. At any time one feels the need to regulate the boundary and persistence of their personal information, they can reconstruct their identity under a new pseudonym identifier. With the change in a context, such as completing the course, a contextual identity may become irrelevant and no longer be used. However reputation earned from A or B updates the over all reputation of Alice or Bob respectively. For details on reputation assessment, update, and transfer, see section 3.8 and 3.9.

3.7 Personalization Support

Since for every information request, a new identity can potentially be constructed based on context and perceived trust, there may be a lack of a persistent marker to aggregate users' behaviors, which is essential to offer personalization. To support personalization, this model suggests the use of sessional tokens to emulate the effect of persistent markers (shown in Figure 3.8): before the end of each session, a new token will be generated for the next session. If a user chooses to receive a personalized service, the user will present that token at the beginning of the relevant session. At the start of each session, the token for the current session expires. For example, at the end of the first session (s0), the token for the next session (s1), token_{s1}, is generated and passed to the information seeker (personalized service provider). At the beginning of the session s1, the information giver (IG) will pass token_{s1} to the information seeker (IS) to allow aggregation of information or attribution of their profile to their identity. Then IG passes token_{s2} for the next session, which invalidates token_{s1} and so on.

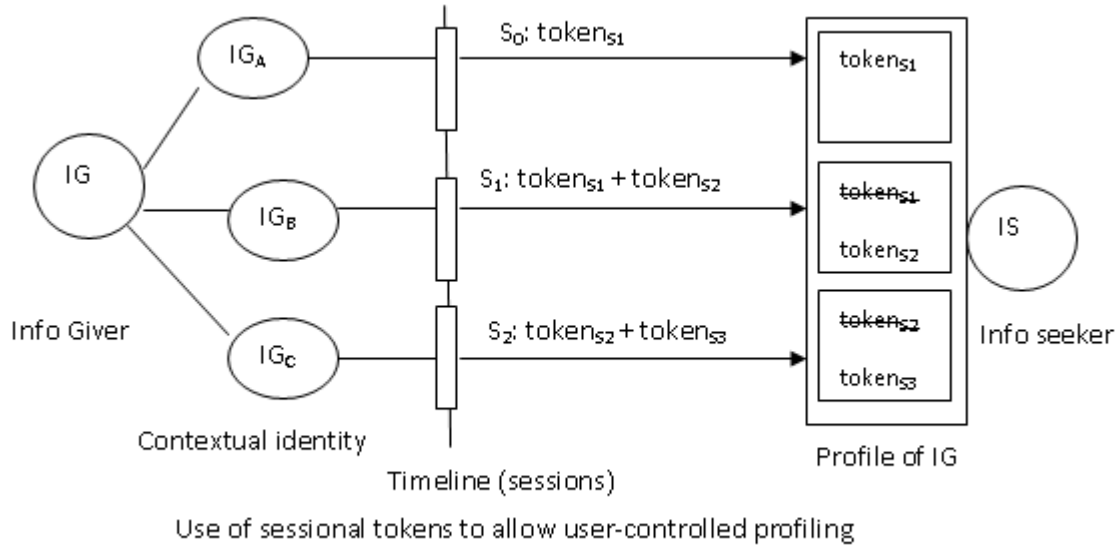


Figure 3.8: Use of sessional tokens as an alternative to persistent pseudonyms

3.8 Reputation Assessment and Update

Generally, reputation assessment involves aggregating observers' opinions on the performance of individuals against the expectations of their roles in similar contexts. However, I realize that context is a nebulous concept. There is no one way to perceive, define, or classify contexts. For the purpose of propagating trust, the similar contexts need to be jointly identified by a user who wants to transfer reputation and a guarantor who oversees the process. Ultimately, the guarantor needs to decide which contexts should be considered similar. The guarantor can be informed by comparing features against which reputation is assessed along the proposed three dimensions of reputation. For example, if competence, benevolence, and integrity in both context A and B are assessed against same features, reputation may be transferable between A and B.

To facilitate formation of an accurate reputation, a system is needed that would: be able to prove itself unbiased and trustworthy, allow individuals to correct or

update their data, be able to judge information in light of time, context, completeness etc., and be able to secure and manage this information. On this regard, this thesis presents a guarantor mediated reputation management system, where the guarantor plays the role of a judge with the above mentioned qualities.

The solution to privacy through maintaining partial identities in different contexts (as in ITMP) can be less appealing due to the fact that reputation earned over a partial identity may be unusable across other partial identities. Since the pseudo-identities and pseudonyms offered by the partial identity solutions by default are not linkable, the complete assessment of reputation can easily be disrupted by switching and shedding of pseudonyms: reputation earned over a pseudonym is unusable with the shedding or switching of that pseudonym. Although a mechanism for reputation transfer across partial identities of a person may address this problem, it may pose the threat of linkability to privacy: by observing a reputation transfer, an observer may be able to link the transferor identity with the transferee identity. Therefore, reputation aggregations/ transfers across multiple partial identities have to happen un-observably and securely. Such a transfer has to restrict any undue advantage for bad acting (e.g., cover up of a bad reputation by recurring merger with a good reputation). To address these limitations of the proposed privacy model, this thesis also presents a guarantor-facilitated, unobservable, secure, and safe (resistant to misuse) reputation transfer model. Another approach is to associate with each person in each context a reputation that persists across partial identities. A new rating for an action of any partial identity updates the reputation.

3.9 Reputation Transfer across Pseudonyms

With the persistent use of a pseudonym (for a partial identity), the attribution of reputation markers to the pseudonym takes place. A pseudonymous actor cannot, on their own, transfer or merge reputation across their multiple pseudonyms, yet such ability is highly desirable. Therefore, a pseudonymous actor needs a privacy-preserving mechanism for the transfer or merger of their reputation across their

multiple pseudonyms.

3.9.1 Secure Reputation Transfer (RT) Protocol

Here I present a secure reputation-transfer protocol, through which an actor registers its partial identities with a guarantor who would vouch for the actor. The guarantor periodically evaluates the reputation of the actor based on their and other community members' observations. After each evaluation, a copy of the reputation is sent to the respective actor. The actor gets an opportunity to contest any misrepresentation of their reputation to the guarantor. The guarantor investigates the challenge and thereafter makes an appropriate adjustment to the reputation. In RT model, there are the following four entities:

- Actor: An actor is a participant (e.g. student, tutor, instructor in an e-learning environment) in a community, who takes part in various activities (e.g. chat, discussion) assuming their various contextual partial identities. The actor can be thought to have 2 partial identities, source and destination.

- Reputation: Reputation is the trustworthiness of an actor assessed over their past activities. For example, Alice may have worked in numerous collaborative course projects in the past. Based on her previous records, she could be trusted as a hardworking participant. However her skills in programming assignments cannot be highly trusted.

- Guarantor: A guarantor is a public actor who is a trusted witness of the past activities of a pseudonymous actor. For example, since an instructor observes a student over a period of time, the instructor can serve as a guarantor of a student's reputation. A trusted system could play the role of a guarantor for its users as well.

- Key Generator: A trusted key generator that facilitates Public Key Infrastructure. This system component provides public/private key pair for the actors and the guarantor without knowing the purpose or usage of the key pairs.

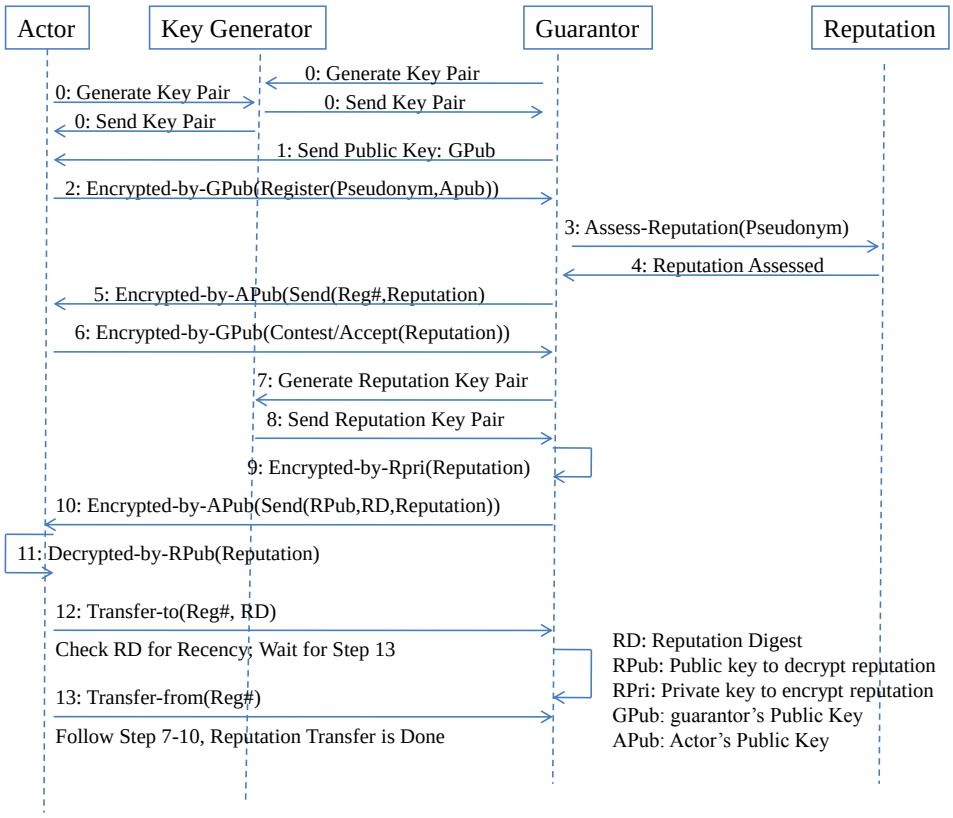


Figure 3.9: A model for reputation transfer across pseudo-identities

The steps of reputation transfer model in Figure 3.9 are presented in the Table 3.1:

Table 3.1: Steps in reputation transfer protocol

Step	Activity
0: Generate Key-Pair	The Key Generator provides (public/private) keys to actors & the Guarantor
1: Guarantor publishes its public key	The guarantor publishes its public key so that any communication to the guarantor is encrypted by the guarantor's public key and thereby secure
2: Pseudonym Registration	A pseudonymous actor registers their two partial identities (e.g. source and destination) with a trusted public guarantor by sending an encrypted request
	The actor also sends its public key to the guarantor so that the actor-bound communication is secure
3 & 4: Generate reputation	The guarantor generates reputation for registered partial identities by aggregating ratings submitted by their transacting partners.
	The reputation earned on a specific feature f is generated as a reputation point average (RPA_f), on a 0 to 5 scale (0 representing unknown and 5 representing the best): $RPA_f = (RPA_f \times \lvert ratings_f \rvert + newrating_f) \div (\lvert ratings_f \rvert + 1)$
5: Guarantor sends reputation to the actor	The actor receives report cards of reputation from the guarantor for each of their registered partial identities so that the actor could contest any misrepresentations or mistakes

Table 3.1: Steps in reputation transfer protocol

Step	Activity
	For each registered partial identity, the actor receives a unique registration number, which will be used to identify a partial identity during the reputation transfer process
6: Contest or accept reputation	An actor could contest and clarify any unfair rating and eventually accept the reputation of a partial identity. The guarantor may adjust reputation on any plausible ground
7 & 8: Generate KeyPair for reputation	The Key Generator provides (public/private) keys to the guarantor for encrypting each finalized reputation
9: Encrypt reputation	Each reputation is encrypted with the reputation private key, RPri
10 & 11: Encrypted Reputation is sent w/ the digest and the public key	The guarantor sends the encrypted reputation and the reputation public key, RPub, so that the actor can decrypt and peruse their reputation (Step 11). However, the actor will not be able to change the reputation
	The guarantor also generates the reputation digest on the public key of a reputation and sends it to the respective partial identity of the actor so that the non-repudiation and the integrity of the reputation is verifiable
12: Transfer reputation (Source's part)	The reputation source (partial identity) initiates the reputation transfer process by sending the reg# (provided at step 5) and the reputation digest (provided at step 11).
	The reg# authenticates the actor, and the digest authorizes the transfer

Table 3.1: Steps in reputation transfer protocol

Step	Activity
13: Transfer reputation (Destination's part)	The reputation destination (partial identity) participates in the transfer by providing its reg#
	The transfer is a two-way process to avoid any forgery
Repeat Step 7-10: Encrypt the transferred reputation with newly generated key sets	After the reputation transfer request is validated, step 7 to 10 are repeated to encrypt the transferred reputation and generate reputation digest for the transferred reputation

In summary, in the RT model (see Figure 3.9), a pseudonymous actor can update the reputation of one partial identity by transferring its reputation from another partial identity. A guarantor vouches for an actor in two ways: (i) responding to the reputation queries about the actor, and (ii) responding to the actor's reputation transfer request from one pseudonym to another.

3.9.2 Restricting Bad Acting in Reputation Transfer

In reputation transfer, an impostor may launch a man-in-the middle attack, impersonating the owner of a particular partial identity or the guarantor. Then the impostor may attempt to steal good reputation from others or may pollute others' good reputation with their own bad reputation. An impostor may change the original reputation of a partial identity. An actor may maintain good reputation on one partial identity and repetitively transfer reputation from that partial identity to other partial identities. An actor may transfer the same good ratings again and again to improve reputation of a partial identity. The RT model provides mechanisms for restricting these types of bad actions in reputation transfer:

- The integrity of reputation can be checked using the reputation digest, a 128-bit "fingerprint" of reputation information generated through the calculation of MD5 hash.

- Since both the transferring and receiving pseudonyms are registered to the guarantor, any bad acting can be traced and verified by the guarantor.

- To restrict the taking of undue advantage from recurring merger of a bad reputation with a good reputation, a history of already merged ratings is kept and compared before entertaining a new merge request.

- The model also supports rollback of reputation to recover from bad acting.

3.9.3 Restricting Link-ability of Partial Identities

Since linking of partial identities results in unintended disclosure defeating the purpose of partial identities, the transfer of reputation among the pseudonyms or update of reputation because of new ratings has to happen without letting anyone link one pseudonym with the other. Privacy protection in reputation transfer further requires that the transfer must occur without letting anyone recognize such a transfer. In the RT model, non-observable and non-linkable reputation transfer is done by means of the following techniques:

- Use of public key infrastructure ensures a secure reputation transfer channel so that an observer cannot snoop a reputation transfer or directly identify two pseudonyms involved in the process of a reputation transfer.

- When a new rating is recorded against an action of a partial identity, it updates the overall reputation of that identity. A reputation transfer process mimics the reputation update process by treating each rating of one identity as a new rating for another identity for both the identities involved in the reputation transfer. As a result, one partial identity's reputation (i.e., aggregated ratings) is incremented one-by-one by each rating transaction of the other partial iden-

tity and vice versa allowing longitudinal increase or decrease in reputation to make transfer indistinguishable from reputation update by a new rating.

- It is very unlikely that new ratings against some behaviour of a partial identity come all at once. A random time delay is induced between each of the increments to make reputation transfer indistinguishable from reputation update by a new rating, which may not happen in a continuous succession of a short burst.

- A time delay proportional to the amount of activities takes place in the system is induced between increments of reputation so that multiple partial identities of an individual are not linkable because of one reputation update triggering changes of reputation of multiple pseudonyms. This will restrict reputation updates in multiple partial identities of an actor at the same point in time. As a result, the partial identities of that actor cannot be linked from observing reputation updates.

3.10 Conclusion

In this chapter, a 3-dimensional characterization of privacy is introduced. It is argued that these three dimensions of privacy can be regulated through the following means: selective disclosure to control flow, restrictions of secondary use to control boundary, and expiration of information to control persistence of disclosed information. A context, trust, and identity based 5-layer model for privacy, ITMP, is presented to provide mechanisms for facilitating selective disclosure, restriction of secondary use, and expiration of information. In this model, contextual trust is used to support selective disclosure (i.e. information flows towards a trustworthy partner). Any disclosed information can be later made unusable (thereby regulating secondary use and enforcing expiration) through disassociating information from its owner. A guarantor-facilitated reputation transfer model, to be used in ITMP, is also presented to make identity reconstruction more appealing, overcoming the limitation of partial

identity through the transfer of reputation across multiple pseudonyms.

Chapter 4

Implementing ITMP in the E-learning Domain

This chapter concerns the use of the ITMP model (and the RT model therein) in supporting selective disclosure of information, information expiration, restriction on secondary use of information, and reputation transfer across partial identities in an e-learning environment. As with any generic model, these models need to be interpreted for a specific domain (e.g., an e-learning domain) without compromising their integrity. For the purpose of validation and verification, the ITMP model was implemented in the iHelp Discussion forum, which acts as an online forum for students at the University of Saskatchewan to converse asynchronously with one another, with subject matter experts, and with their instructors. The RT model is implemented as a stand-alone client/server simulation application emulating reputation management in a learning environment.

The conceptual background section below refreshes the readers of the various components of the ITMP model and interprets these components to operationalize them for the e-learning domain. In implementing the ITMP model, a role- and relationship-based identity management scheme was introduced for iHelp. The implementation is illustrated by means of various use case scenarios together with a series of screenshots. Finally, I discuss how the implementation of the proposed model in iHelp Discussion (a component of an e-learning environment) addresses the central research questions, which have emerged in this thesis.

4.1 Conceptual Background

In consideration of promoting a privacy-preserving information sharing paradigm, a 5-layer identity and trust based model for privacy (ITMP) has been presented in Chapter 3. Besides the input and output layers (i.e. application and presentation), three of the principal components (layers) of this model are context, trust, and identity. Combined, these three components help users manage privacy supporting trust-based decision making and separation of identity from behavior. Additionally, users can request and use personalized services based on their respective observable behaviors. Therefore, the context, identity, and trust components of this generalized model need to be interpreted for the e-learning domain in order to apply the model in the iHelp Discussion Forum.

4.1.1 Context

In the ITMP model, roles of and relationships among individuals are used to capture the notion of context to address their privacy. Each context explicitly or implicitly manifests some purpose for its participants. Based on the purpose, a participant assumes an appropriate role or engages in a relationship. In an e-learning system, participants subscribe to various roles: learners, peer coaches, markers, tutors, and other learning support staff. In various contexts, each participant of an e-learning environment engages in the following type of relationships: one-to-one, one-to-many, many-to-many, and hierarchical.

In a one-to-one relationship, two participants want to be identifiable to each other and distinguishable from other participants. In a one-to-one relationship, the participants share personal information warranted by the role and purpose of the one-to-one relationship. In a one-to-many relationship, a participant wants to communicate with a group of actors (e.g., discussants in a forum) in the same manner. In a one-to-many relationship, for example, an instructor in a course wants to inform all the course registrants about course materials. For this kind of purpose, the entire class may subscribe to a group identity. A many-to-many relationship can be bro-

ken down into two one-to-many relationships: in a student-instructor many-to-many relationship, a student enrolls in multiple courses from different instructors and an instructor teaches different students in multiple courses in a semester. A hierarchical relationship serves to define a hierarchy. For example, a student in a marker role grades other students' work. An instructor working as a department head supervises other instructors.

4.1.2 Trust

Based on the observation that privacy and trust hold a symbiotic relationship, the ITMP model uses trust to manage privacy. The model postulates that managing privacy involves a trust-based decision-making process when sharing personal information. A pseudonymous actor, who has acquired a favorable reputation, gains the trust of other actors. In a well understood context, individuals may share their identity with a trustworthy information seeker. To facilitate reputation-based trust (i.e., trust is associated with the reputation of an actor), the trust layer of the model needs to support complete assessment of reputation across partial identities. As a result, this model incorporates a secure and privacy-preserving reputation transfer (RT) model [Anwar and Greer, 2008a, Anwar and Greer, 2006] in order to transfer/merge reputation across contextual partial identities in the trust layer. Given that the purpose and the partner are trustworthy, the identity layer constructs a contextual partial identity from a complete identity.

In the RT model, a pseudonymous actor can update the reputation of one partial identity by transferring its reputation from another partial identity, effectively merging reputation across partial identities. Though anonymity does not support building of reputation, sometimes a pseudonymous actor needs to act anonymously. For example, in a course discussion group, a shy student, Bob may want to be anonymous when conversing with peers about some research ideas, whereas that student may want to be recognized as *BobTheHelper* when helping peers. Yet if a favorable reputation provided by a trusted source could be associated with an anonymous actor, the actor could enjoy appropriate credibility. For example, despite anonymity, a

high competence score associated with Bob's anonymous identity may attract other students to converse with him.

In the RT model, a guarantor (an appropriate public trusted actor) vouches for a pseudonymous actor in two ways: (i) responding to the queries about the actor's reputation, and (ii) responding to the actor's reputation transfer request from one partial identity to another. The reputation is generated as a reputation point average (RPA) on a 0 to 5 scale, 0 representing unknown and 5 representing the best. The guarantor generates reputation for its registrants (i.e., pseudonymous actors) by aggregating ratings submitted by their transacting partners. In the e-learning domain, instructors, with the aid of privacy-enhanced reputation management (e.g. reputation evaluation, reputation transfer/merger) tools, can play the roles of guarantors and adjudicators of their students' reputations.

To provide a solid and parsimonious foundation for the empirical study of trust for another party, Mayer et al. [Mayer et al., 1995] observe three characteristics of a trustee appearing often in the literature: ability, benevolence, and integrity. For learners, reputation is a mechanism for ascertaining the trustworthiness of participants, analogous to those in eBay. Therefore, using trust as a scale to find a suitable recommender, peer, helper, and mentor, a learner should be able to find out the status of each participant in an e-learning environment: is someone really the expert or well-intentioned peer that they claim to be? One can also decide whether trust can replace the need for privacy: can one confide in their peers? Most importantly, in generating reputation of a learner, their behavior has to be evaluated (not their identity) by their transacting partners.

4.1.3 Identity

An identity is a union of various partial identities of which each represent a person in a given role through a dataset that holds information such as attributes (name, student number), traits (biometric information), and preferences (food choices, learning styles) [Anwar et al., 2006]. At the identity layer, the ITMP model constructs a partial identity for an individual by grouping context-relevant information under

a transactional identifier. Partitioning a complete identity along contexts (primarily represented through roles and relationships as shown in Chapter 3) keeps the amount of information revealed to minimum (thereby contributes to privacy) without disrupting the desired flow of information. An individual holds multiple partial identities in different contexts. Each partial identity (a contextual identity) can be presented with many different identifiers or pseudonyms. However, an actor in a specific role can be or a relationship may need to be identified by the use of a persistent pseudonym.

Since the roles (e.g. instructor, learner, marker, administrator, etc.) for participants are well structured and relationships (e.g. one-to-one, one-to-many, hierarchical, etc.) among roles are relatively predictable in the e-learning domain, a role- and relationship-based identity management scheme is a natural instantiation of the ITMP model. In this approach, a role-level identity hides an actor in the crowd of actors of the same role, and a relationship-level identity allows an actor to disclose information appropriate for a respective relationship. Sometimes, a context-level identity is more appropriate for an actor of one context (a guest) to be presented in another context (a host context). For example, an instructor of a follow-up course may use a context-level identity while conversing with students of a pre-requisite course. Moreover, actors of public roles (e.g. instructor in a course, disciplinary committee in a department, etc.) can be assigned guarantor privileges to sanction foul acting and to facilitate usage control over disclosed information.

4.1.4 Role- and Relationship-based Identity Management (RRIM [Anwar and Greer, 2008b])

The ITMP model negotiates an appropriate identity for a user, taking inputs regarding "who is who", "what their purposes are" and "how trustworthy they are" in an information sharing context. After introductory communication initiated by the application layer of the model at both users' (i.e., information seeker and information giver) ends, the purpose, partner, and information sought are identified.

The context layer helps understand the communicative context in terms of role of and relationship with communicating partners. For a well defined context, the trust layer measures the trustworthiness of the partner. The identity layer constructs/ negotiates an appropriate partial identity for the potential information giver (based on their role and relationship with the information seeker so that a desired level of privacy can be achieved).

Explicitly or implicitly, each context serves some purpose for its participants. Based on the purpose, a participant assumes an appropriate role or engages in a relationship. A role can be defined as an expected behaviour attached to the position of an individual in a community. For example, in a learning community, an individual in a teaching role is expected to set learning objectives, give lectures, evaluate students' performance, etc. Likewise, an individual in a basic learner role is expected to enroll in a course and undertake course related activities like attending lectures, asking questions, participating in course evaluation, etc. A relationship is a specific connection manifested in individualized interaction between two roles. For example, in an advisor-advisee relationship, a teacher engages in personalized communication with a student for guiding the student during their academic career. Or, an individual in a student role may engage in a peer relationship with a lab-partner drawn from individuals of the same role (student) in a specific course context.

I defined a purpose-based and recursive notion of context in the e-learning domain (shown in Figure 4.1). For a well-defined purpose, each participant creates a context by assuming some type of role and negotiating some type of relationship. Sometimes, all the participants may play just one role - their affiliation to a context (e.g. passengers in a wait queue). Each context exists until its underlying purpose is achieved. Since each role or relationship is contextual, any role or relationship is not valid any longer than that of the relevant context. A context may spawn another more granular context, which in turn may spawn yet another context and so on. A context rewinds all its descendant contexts before it comes to an end. A participant in a context may use either their context-specific temporal (i.e. while the context lives) identity or more generic identity from any of its progenitor (super)

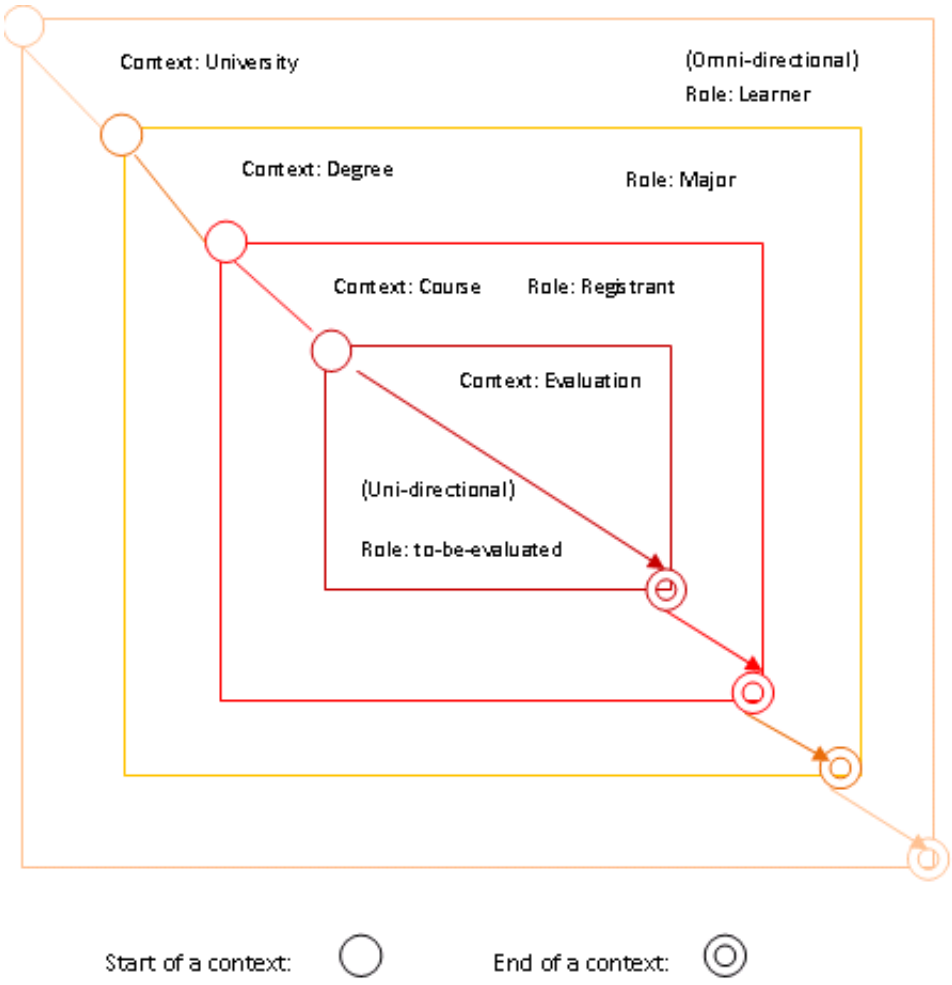


Figure 4.1: Contexts of various granularities in an e-learning domain

contexts. For example, in a Computer Science course context, a student may use their context-specific role-based identity of type "course registrant", or the student may choose to use more generic role-based identity of type "CMPT-major" from the degree context (i.e., progenitor of the course context as shown in Figure 4.1).

In building a role and relationship-based identity management system, the following tasks are identified: identifying relevant roles for different contexts, crafting role-based identities to be used by each participant of a role, allowing each participant to assume multiple roles as they qualify and to switch between roles, facilitating the creation of relationship-based identities for roles to build justifiable relationships, and allowing a guarantor to link historical data to its owner to make them accountable for their actions. A representative role- and relationship-based identity management

system should facilitate the creation of a context for a purpose (e.g. a course context for the offering of a course CMPT111), roles for various job functions of participants in a context (e.g. a registrant role in the context of Course - CMPT111), and relationships for various job functions among roles (e.g. a supervisor-supervisee relationship between an instructor and a marker role). After authentication, the system should generate a context hierarchy for a participant, in which each context-node corresponds to the affiliation of the participant in a context, and thereby, represent a context-level identity.

Once roles are identified (i.e. a set of tasks expected of a role to perform in a given context is grouped under a role name), a role-based identity creation involves assigning an actor to a pertinent role, generating a role-term pseudonym for the actor on the assumption of a role, and creating an identity dataset consisting of only role-specific information. Based on their assumed role within a context, the system should allow one participant to choose an appropriate relationship with another participant, help a participant create a relationship-specific identity dataset, and generate a relationship-term pseudonym for the participant to be used in a relationship. For providing awareness cues to a participant, the system should display the hierarchy of contexts relevant to them together with their assumed roles and relationships therein.

Even though a role-based identity from one context can be used in all the descendant contexts, a relationship-based identity in one context is likely irrelevant in another context. For example, instead of using her context-specific pseudonym as a registrant of a course, *registrant43*, a student may choose to appear as *cs37*, revealing her affiliation with the Computer Science department. Other enrollees of that course would not know whether *cs37* is a co-registrant in the respective course, an instructor of this course, or a student in the department who may or may not be enrolled in that course. When *cs37* seeks technical writing help from the learning centre and creates a relationship-based identity with a writing tutor, she reveals more personal information. Due to the temporal dimension of role or relationship, any information released under a role or relationship ought to be virtually unusable

for the counterpart when the respective role or relationship expires. Anytime, a participant fears a privacy threat in a relationship-based identity, the participant may abandon their respective relationship-based pseudonymous identity and take refuge in their role-based identity. The participant can negotiate a new relationship at any time and craft a new relationship-based identity.

Ideally, a relationship-based identity is constrained by the purpose of a relationship, which in turn is constrained by the context of the relationship and contextual roles of the participants involved in that relationship. A relationship should not blow the cover of a role, and the identity revealed in a relationship in one context should not be linkable to another context. Since all the participants in the same role carry the same role-based identity, the role-based identity approach provides a degree of anonymity to the participants of a role.

Illustrated in Figure 4.2 is how the idea of role and relationship-based identities work in a scenario in the learning domain. Entering at the university, Alice subscribes to a student role. Accepting a faculty position, Bill subscribes to a faculty role. In the advising context, Alice and Bill engage in an advisor-advisee relationship as *Advisor03* and *Advisee43*. Alice presents herself as *Registrant56* and *Examinee23* at the course context and at the evaluation context respectively. In this scenario, role-level identities are the following: *student, faculty, advisor, advisee, registrant, examinee*. Bill and Alice are entitled to the following context-level identities, where their roles are shadowed: *Advising, Course, Evaluation*. Relationship-level identities for Bill and Alice are the followings: *Advisor03, Advisee43, Registrant56, Examinee23, Instructor07*.

The creation and maintenance of so many role- and relationship- based identities may seem like daunting tasks for participants. However, for each user account, the system should perform context and role assignments providing a default role-based identity for each role that the participant may partake in. The system can also enable participants to engage in likely relationships (determined by their assumed roles in respective contexts) and provides relationship-based identities. For example, in a course context, the system should enable a registrant to create a

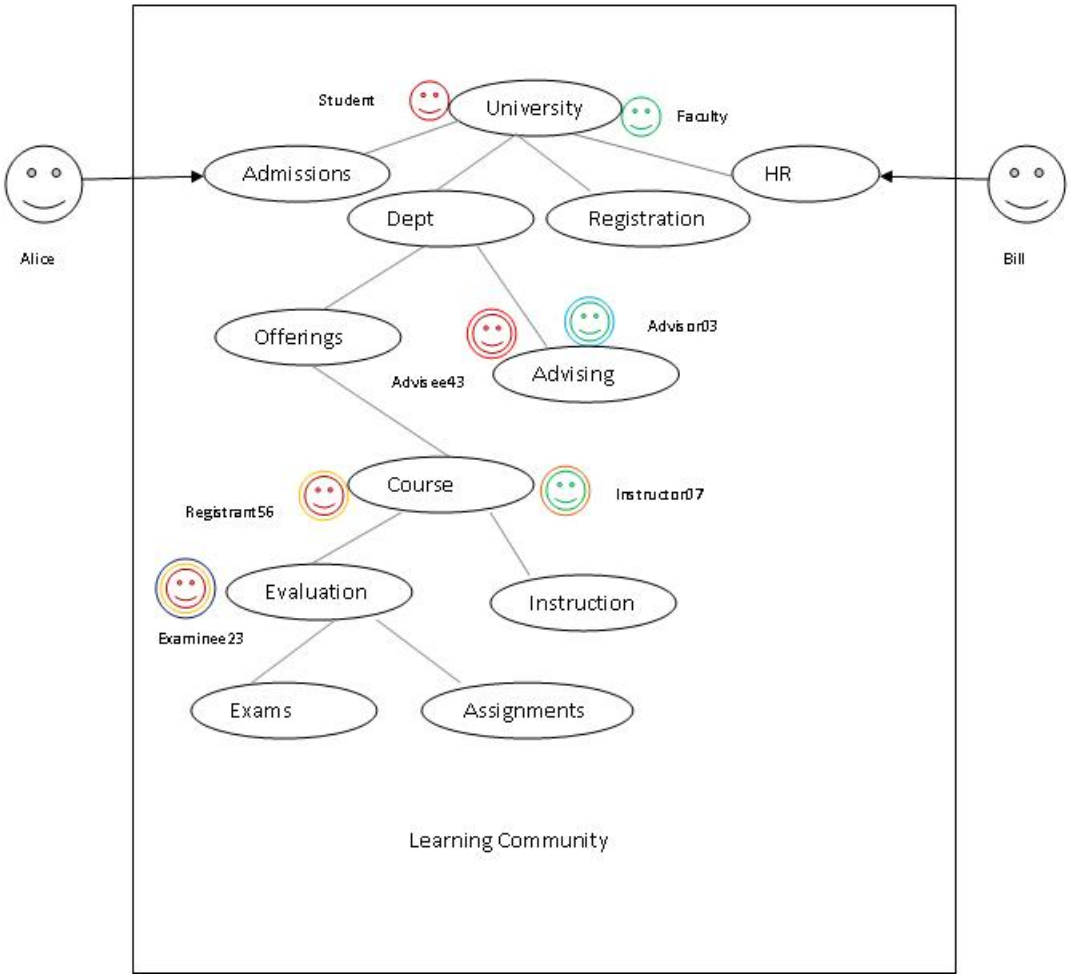


Figure 4.2: Identities of Alice and Bill at various contexts

persistent relationship-based identity to be used to manage a relationship with the course instructor. To help users manage their identities, the system needs to provide awareness to participants through visualization of contexts, roles, relationships and pseudonyms of them and their partners. Additionally, the system should enforce expiration of context, role, or relationship and track information for a cause, which is deemed justifiable by a guarantor.

4.2 ITMP implementation in iHelp Discussion System

The iHelp Discussion[1] is a component tool of the iHelp Online Learning System. The iHelp Discussion tool serves as a discussion medium for students, markers, tutorial assistants, instructors, guests, etc. The iHelp Discussion system has wide use throughout the Computer Science curriculum at the University of Saskatchewan. This system integrates with the existing academic role structure in courses to seamlessly support the various kinds of users (students, markers, tutorial assistants, instructors, etc.) and the permissions and needs that they have with their courses. Postings fall into categories (e.g. Midterm, Module1, etc.). It facilitates context separation by providing context specific interaction categories. For example, the iHelp Discussion category under the heading of CMPT_350-Assignment_1 would be open only to students in CMPT 350 as well as the instructor, teaching assistants, and other potential helpers. Learners post and respond, seeking help and offering help, and instructors can do the same.

Previously, in the iHelp Discussion System, participants have the option of posting either anonymously, or using their real name (i.e., first initial followed by lastname), or using any of their up to four self-created aliases. In implementing the ITMP model in iHelp, various privacy features are added to iHelp Discussion in order to realize the following objectives:

[1] http://ihelp.usask.ca/discussion

- help participants manage their context and role specific partial identities
- enable participants to rate other users based on their postings (ensuring separation of true identity from behavior)
- help participants manage their reputation for their multiple partial identities

The added RRIM and reputation features (shown in Figure 4.3) of iHelp Discussions are implemented in Java, JSP, JavaScript, DHTML, HTML, and XML that use a MySQL database at the backend. The implementation makes extensive use of asynchronous JavaScript (i.e., AJAX) and DHTML to realize the interactive markup effects. In the implementation, the system plays the role of a facilitator of identity and guarantor of reputation.

4.2.1 Context Tree

In Figure 4.4, the sidebar of the iHelp Discussion window (screenshot) shows a context- and role-level identity tree of an iHelp discussant. A discussant participates in a context in the capacity of their various assumed roles. For example, in the Figure 4.4, the discussant could participate in Net Neutrality context in the capacity of **Proponent** or **Opponent** roles. A discussant's identity is partitioned into multiple partial identities under various contexts, sub-contexts, and roles.

A discussant can have three types of pseudonyms to represent their various partial identities: user-level, category (or context)-level, and role-level. A user-level identity provides a discussant one identity for all different contexts. For example, **BobTheDiscussant** pseudonym for a user-level identity allows a participant to maintain publicity across various contexts or sub-contexts. Both the category-level and role-level identities can be represented by a generic (or group) pseudonym or a user-defined (or individual) pseudonym. In the Figure 4.4, **ABR#** is a category-level generic pseudonym, which makes a discussant indistinguishable from other discussants in the discussion context of Abortion. It also provides the discussant a group identity. On the other hand, **Opponent#** is a role-level generic identity representing the discussant as a member of the group of individuals in Abortion-Opponent role.

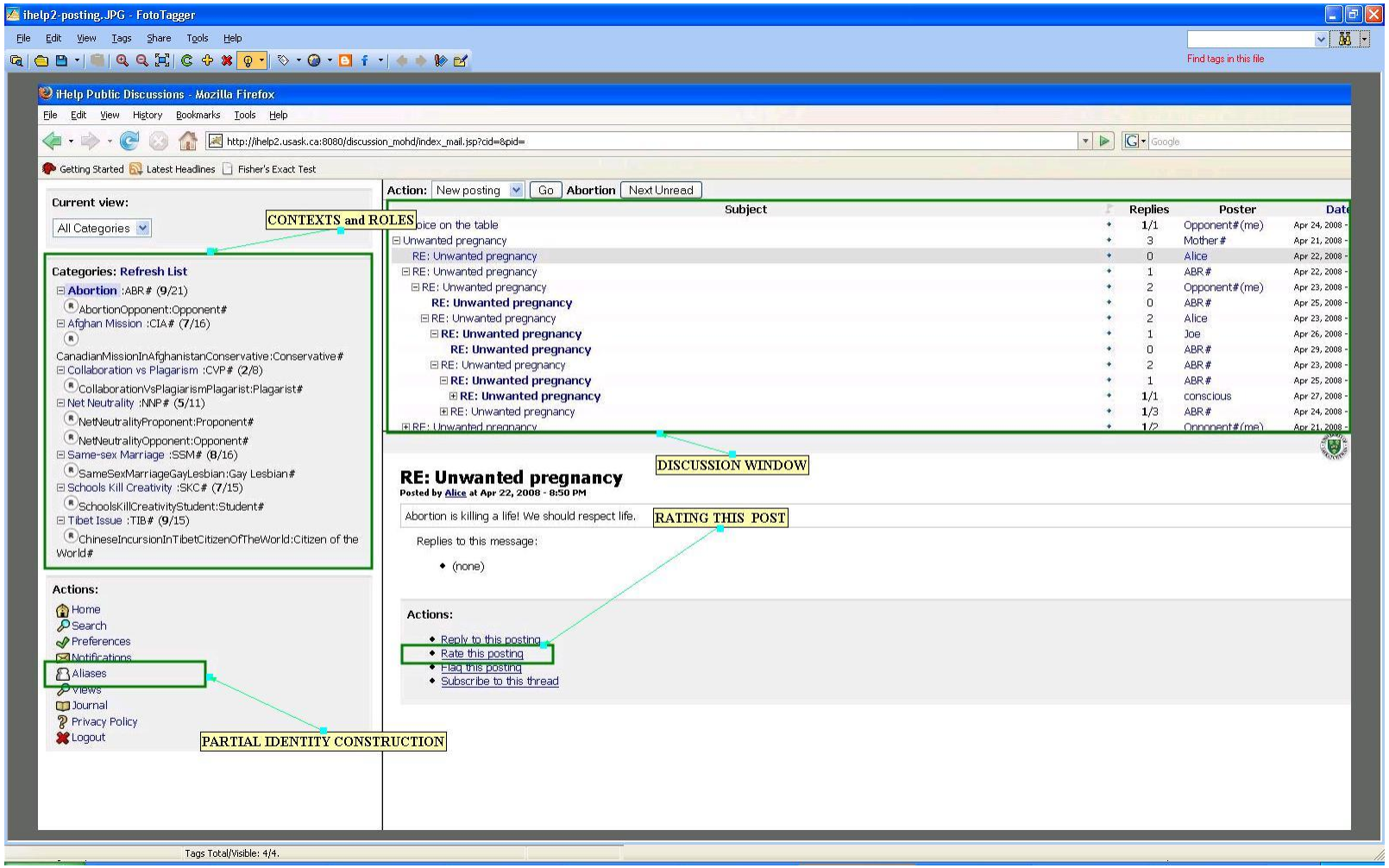


Figure 4.3: Screenshot of a iHelp discussion page

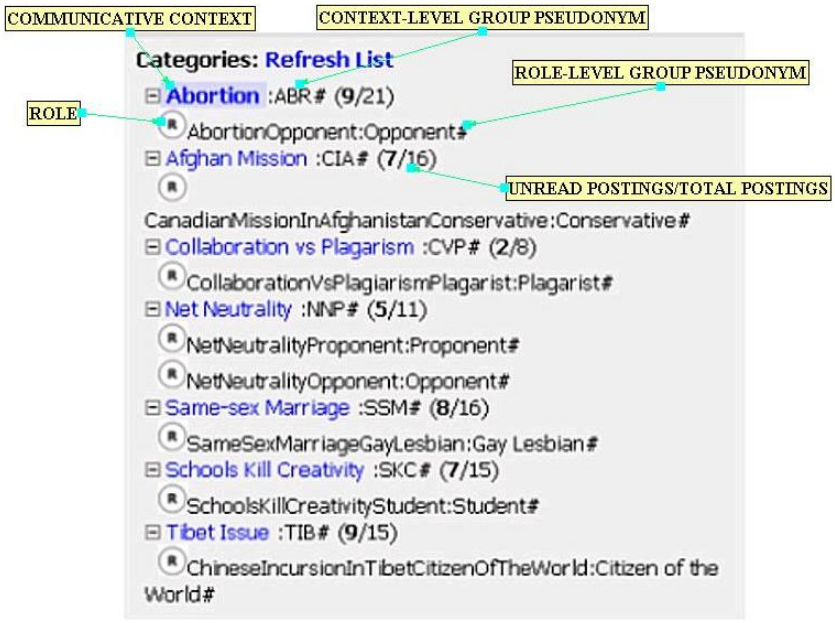


Figure 4.4: Context hierarchy presented in iHelp discussion

A user-defined category- or role-level pseudonym allows a participant to be distinctive. This type of pseudonym can also be viewed as a relationship pseudonym since the discussant uses this pseudonym to represent an identity to negotiate relationship with other discussant in a context.

4.2.2 Privacy-preserving Selective Disclosure

Illustrated here is how the idea of RRIM facilitates context-dependent selective disclosure of identity. The system implementing RRIM constructs different purpose-based communicative contexts for the actors in a particular domain. Since an actor assumes a distinct role or engages in a relationship in a communicative context, the system creates various roles and assigns roles to actors. The system provides context- and role-level group identities to each participant of the respective contexts and respective roles. Additionally, the system allows its actors to create their distinctive relationship-level partial identities. The system allows an actor to assume and help them manage their different partial identities to communicate within and across contexts. As shown in Figure 4.5, the system identifies the context of a post and allows a participant to choose from a list of context-appropriate partial identities

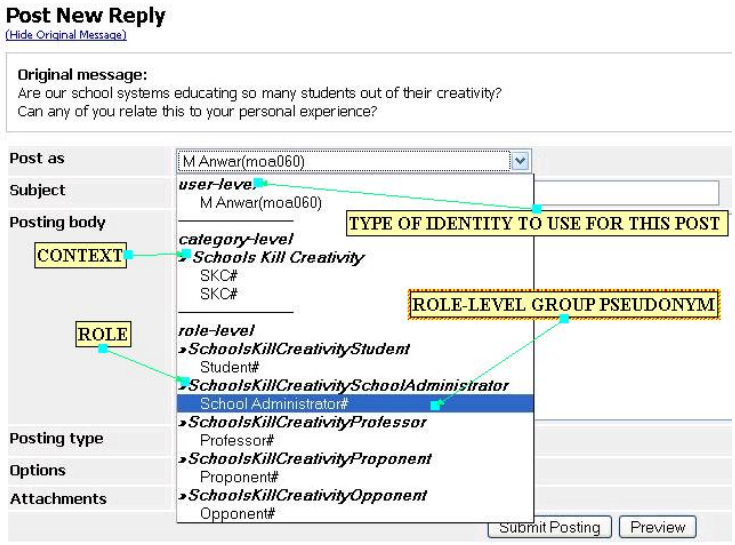


Figure 4.5: Reply to a posting using an appropriate identity (screen shot)

in replying to a post. As a result, the system effectively partitions an identity into multiple partial identities along various contexts, roles, and relationships.

4.2.3 Privacy-preserving Identity Management

In RRIM, the context of identity is captured through purpose, role, and relationship. Each purpose initiates a potential context for an identity. For example, for the purpose of discussing about Tibet, a discussant joins Tibetan Issue group. In the discussion group, the discussant may play the role of the chinese government to present the chinese government's perspectives on the issue. The discussant has two types of identity choices: individual and group (e.g., in Figure 4.5, M Anwar is an individual identity, and Professor# is a group identity).

Using individual partial identities, a discussant conveys their distinctive presence in the group. The discussant may want to differentiate their action from others. They may want to be recognized or take credit for their actions. Using an individual partial identity persistently, one could establish a relationship with other discussants. Therefore, an individual partial identity can be termed as a relationship-based identity. A relationship-based identity is of two kinds: context-level and role- level. Using

a context-level or role-level relationship-based identity, a discussant conveys both his association with the respective context or role and his individuality.

Illustrated in Table 4.1 are the types of identities available in RRIM. In a group identity, the discussant is indistinguishable from other group members. Using a context-level group identity, a discussant conveys their affiliation (or belonging) to a context to other discussants. Using role-level group identity, the discussant conveys to other discussants that he is one of the many discussants who supports, say the chinese government role. Instead of using multiple fragmented identities, a person may also choose to use a monolithic user-level or global identity.

Table 4.1: Types of identities and their instances

identity-type	group-scope	individual-scope
role-level	a Tibetan-Independence-Supporter	Joe-Tibetan-Supporter
	a Chinese-Government-Supporter	Mary-for-Chinese-Establishment
context-level	a Tibet-Issue-Discussant	Bill-in-Tibet-Issue
	a Olympic-Games-Discussant	Alice-in-Olympic-Games-Issue
relationship-level		Bill
		Marry
user-level (global)		Jim Greer
		Mohd Anwar

Based on the context and role of participation, each participant is provided with pseudonyms to represent their different context- and role-based group identities. The system also provides each participant with a pseudonym to represent their user-level global identity, which can be used to participate across roles and across contexts.

Additionally, the system provides tools for participants to construct individualized (relationship-level) identities (and respective pseudonyms) to initiate and maintain a relationship through the use of that persistent identity in any given context or in any given role (shown in Figure 4.6). In replying or posting new messages, participants are presented with their pseudonyms to choose from, representing all the pertinent identities under a given context. To help participants identify their own postings, even when group identities are used, each of their own posting carries a **(me)** marker next to the poster's pseudonym. When a role-level individual identity is used, the role name followed by a **(me)** marker is attached next to the poster's pseudonym to make the poster aware of the role they assumed in posting a particular

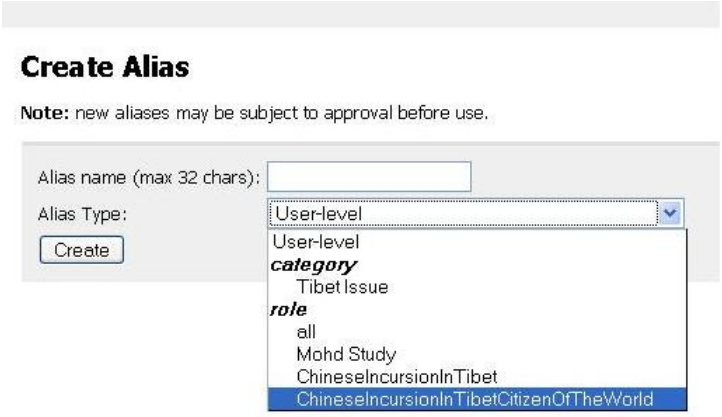


Figure 4.6: Creating individual pseudonym for an identity (screen shot)

message. As a result, it helps participants maintain the integrity of their identities in their postings through awareness. The integrity of identity helps maintain privacy by making multiple partial identities non-linkable.

4.2.4 Privacy-preserving Reputation Evaluation

Since I view identity and reputation being integrally related (shown in Chapter 3 Figure 3.7), a reputation management component is incorporated into RRIM. In RRIM, a person's actions are fragmented along their context, role, and relationship-based partial identities at individual and group capacity. Since, like identity, action should not be judged out of context, reputation is contextual. For example, a graduate student in a researcher role may not carry as prominent a reputation as he might in a tutor role. The trustworthiness of a pseudonymous actor can be computed in a privacy preserving manner by measuring reputation on various aspects of trust pertinent to an actor's specific role in a learning domain. RRIM views reputation evaluation as a process of aggregating observers' opinions on the performance of individuals against the expectations of their roles in similar contexts.

Since all these different identities represent different aspects of their projected self, each partial identity can draw a contextual boundary of an individual's actions, and therefore, each partial identity can serve as a context for reputation as well.

As a result, I view that it would be appropriate to assess actors' reputation on their action partaken under their contextual partial identities. However, I view that actors' actions under group identity should be accounted to both their group's and their individual reputation.

The implemented system assesses reputation of an identity along the dimensions of competence, benevolence, and integrity. In order to calculate each dimension of reputation for an identity, a list of matrices of different weights are presented to a rater to rate an action. In the iHelp implementation, anyone but the poster who is authorized to read a posting is eligible to rate the posting. The rating contributes to the reputation of the poster. Finally, the weighted sum of all the relevant ratings are averaged to calculate reputation along a respective dimension. The system requires raters to judge postings against any (as many as apply) of the six different objective features (shown in Figure 4.7): insightful, timely, informative, well-written, constructive, and relevant. My contention is that it will help participants to be analytical on the postings (i.e., poster's behavior), not on the posters (i.e., poster's identity). This type of separation of identity from behavior contributes to privacy.

I have classified these features based on their impacts (i.e., weights) on determining the level of competence, benevolence, and integrity of a poster. In this implemented system, weights on features are arbitrarily assigned. For example, in determining competence of a poster, an insightful or an informative posting has twice as much impact as a well-written posting. Reputation of an identity is estimated by averaging the weighted sum of relevant features. In calculating final scores, these ratings against relevant matrices are weighted and averaged:

$$R_{competence} = (\sum Rating_{insightful} * weight_{insightful} + \sum Rating_{informative} * weight_{informative} + \sum Rating_{well-written} * weight_{well-written})/number - of - ratings$$

$$R_{benevolence} = (\sum Rating_{constructive} * weight_{constructive} + \sum Rating_{relevance} * weight_{relevance})/number - of - ratings$$

$$R_{integrity} = (\sum Rating_{constructive} * weight_{constructive} + \sum Rating_{timely} * weight_{timely}) / number - of - ratings$$

Ratings on a posting made using a group identity contribute to the reputation of that group identity as well as to the reputation of the poster's individual identities. This is a type of reputation transfer across pseudonyms.

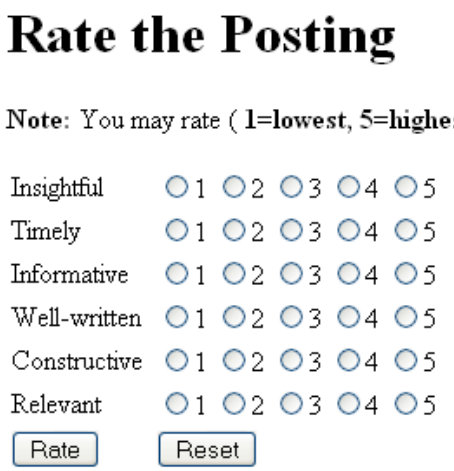


Figure 4.7: Features of rating a posting (screen shot)

As a context ends, the reputation of an identity under that context may be propagated back to its parent context resulting in a backward propagation of reputation from the innermost context to the outermost context. For example, in the outermost context, a person becomes a student for the purpose of attaining a degree. In the innermost context the student is evaluated in an assignment of a course, the student's mark in that assignment is propagated to its parent context of the course and the course grade is eventually propagated backwards to the outermost context contributing to achieving their degree.

4.2.5 Privacy Preserving Yet Accountable Identity Management

Privacy without accountability is counter-productive. We expect not to be accountable to others about an action that does not concern others. However, some degree

of accountability is critical in action performed that affect others. While seeking privacy, it is appropriate to demand accountability in the dealing of our personal information. In relation to identity management, anonymous and pseudonymous actors may need to be held accountable for their actions. Full anonymity without any accountability will engender some socially undesirable behavior.

Even though in the ITMP model, participants can disassociate themselves from their role or relationship based identities, they ought to be barred from doing so in case of any questionable action, while an investigation is launched by a participant holding a role with guarantor privileges. The roles perceived as holding the responsibility of a public trustee by other roles (e.g. an instructor in a course) are granted guarantor privilege. As part of a sanction, a participant found guilty of foul acting may be subjected to identity imprisonment. By demonstrating satisfactory conduct, the participant can be granted digital forgiveness. These ideas about managing accountability are speculative and have not been implemented or evaluated in this research. Yet they are raised for future consideration. These concepts are explained below.

Identity Imprisonment

During communication between two actors, as soon as one actor senses some inappropriate actions by the other, the former could have the guarantor lock the identity of the bad actor. In the locking process, complaints against the bad actor are filed to the guarantor of the respective context, and in response, the actor's activities are monitored. Additionally, the bad actor will be restricted to change their existing pseudonym unless the bad actor is acquitted from complaints, or they have earned good reputation over a period of time. The victim may disown any information disclosed to the bad actor by choosing an indistinguishable role based group identity. Since the victim of the bad acting can identify and reject the bad actor, restricting the change of pseudonym is a sanction to the bad actor without revealing their true identity. In this way, the penalty for bad action is being condemned to an identity that cannot be shed.

Digital Forgiveness

On the other hand, by self-correcting and displaying good behaviour over a period of time, the bad actor can have the guarantor unlock their pseudonym with the bad reputation marker and let them choose a new identity to be free of their past. Once an actor is allowed to disown their guilt-ridden identity, they are forgiven. Other participants will no longer be able to identify the participant as someone who acted inappropriately towards them in the past.

For example, a tutor notices the act of flaming by a student Alice during the online discussion on assignment1. The tutor locks this identifier (i.e. Alice) and thereby reports to the guarantor of this context (i.e. the instructor) about the questionable act. Upon investigation, the instructor may lock the Alice identity for next two weeks that allows the tutor to monitor Alice very closely for any further act of flaming. As Alice demonstrates good behaviour in the next two weeks, the instructor will unlock the Alice identity and allow the participant to assume a new identity. As a result, the participant of Alice identity will be forgiven for the transgression.

4.3 Implementing the Reputation Transfer Model

The trustworthiness of a pseudonymous actor can be computed in a privacy preserving manner by measuring reputation on various aspects of trust pertinent to an actor's specific role in a learning domain. This section presents implementation of role-specific reputation assessment on a partial identity and an implementation of a secure reputation transfer protocol (the details of the algorithm are presented in Section 3.9) to allow reputation transfer among multiple pseudo-identities (e.g. pseudonyms) without letting anyone draw associations among these pseudo-identities. As a result, the implemented system facilitates both privacy and trust.

The prototypical system incorporating the RT model is implemented through a client (for actors) and a multi-threaded server (for guarantor) written in Java language. The Key Generator entity of the secure reputation transfer protocol is implemented using the RSA key pair generation algorithm provided by Bouncy Castle

[2]. The model was implemented using JRE 1.5 and java.security and javax.crypto APIs. The system manages reputation for 3 different generic roles that are present in an e-learning community: helper, peer, and lurker. The system allows an actor to perform any of the following 4 tasks: **register** (i.e., register a pseudonym with a guarantor), **evaluate** (i.e., rate an actor), **transfer** (e.g., transfer/merge reputation across pseudonyms), and **query** (e.g., query reputation of a pseudonymous actor).

- Register: An actor registers with a guarantor who (they trust to be/is) an unbiased public actor capable of collecting, interpreting, and securing their reputation based on ratings from various sources. The communication between an actor and a guarantor is cryptographically secure. At the time of registration, an actor provides their pseudonym and context (role for which the actors want to be evaluated for reputation)(shown in Figure 4.8). Upon registration, the actor receives 2 pieces of information to be kept secret: 128-bit unique registration number and a digest (MD5 hash) for reputation. The digest gets regenerated along with any change in reputation.

- Evaluate: Any actor can evaluate others (i.e. pseudonyms) against the attributes specific to the role of the actor being evaluated on a scale of 0 to 5. Additionally, an evaluator may write supporting comments for their assessment of reputation (shown in Figure 4.9).

- Transfer: Reputation transfer is a two way process that has to be carried out by both the pseudonyms — Source# and Destination#. First, the Source# and then the Destination# authenticate themselves by providing their respective contexts, registration numbers and reputation digests (shown in Figure 4.10). Reputation from one pseudonym can be transferred to a new pseudonym, or reputation of one pseudonym can be merged with the reputation of the other pseudonym. Reputation merge takes place incrementally by combining each rating transaction of a pseudonym one-by-one to the aggregate rating of the

[2]http://www.bouncycastle.org/

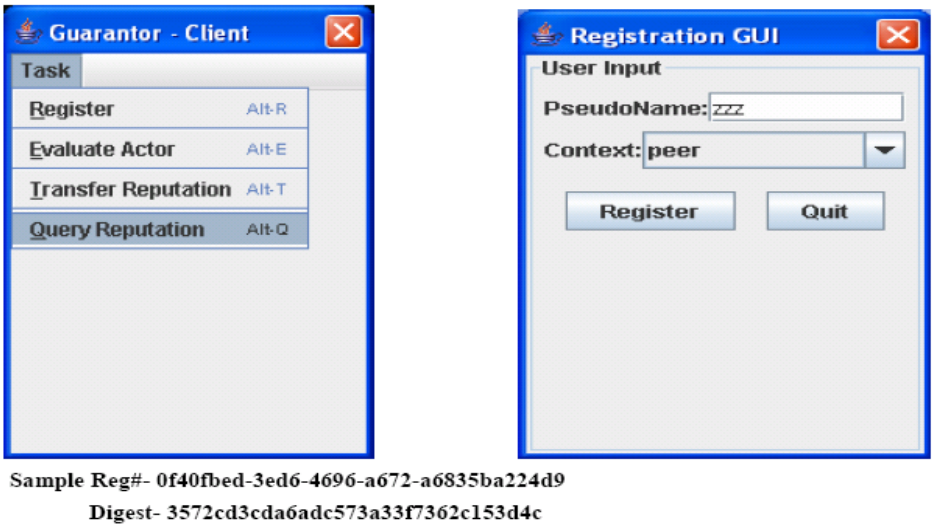


Figure 4.8: Screen shots the reputation management system [client side] menu (left) and registration window (right)

other pseudonym and vice versa. Though the end result of the merge is 2 pseudonyms with the same reputation, their reputations are different on each time step of the merge. There is a little time delay induced in between each step to give the impression that there could have been another transaction (evaluation) taking place.

- Query: An actor may query reputation about another actor (corresponding pseudonym). A reputation summary, which is an aggregation of collected ratings against context-relevant features, is displayed in the following format: *Feature* |*Score* |#*Trans* (i.e., number-of-ratings)".

The implementation was tested in the local host by creating a guarantor object and multiple actor objects. The guarantor and actors had separate repositories in which to keep reputations. The reputation file was generated as a predefined text file of relevant ratings for a given role. Any two pseudo-identities involved in reputation transfer are not linkable by any third party, since the communications between the guarantor and a pseudonym are encrypted using each other's unique public keys. Each of these pseudonyms receives a unique registration number (e.g. 0f40fbed-3ed6-4696-a672-a6835ba224d9). As a pseudonym, say *TomTheHelper* re-

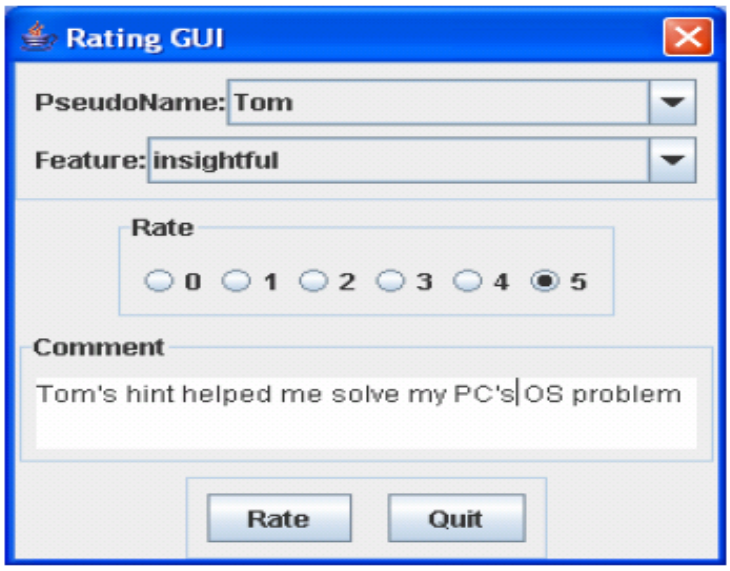


Figure 4.9: Screen shot of a rating window in a reputation management system [client side]

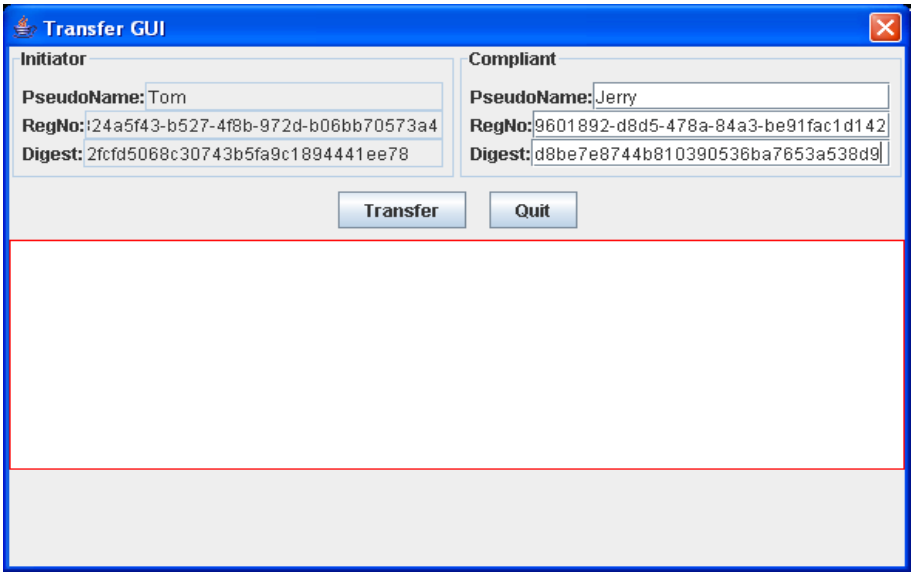


Figure 4.10: Screen shot of reputation transfer/merge request window

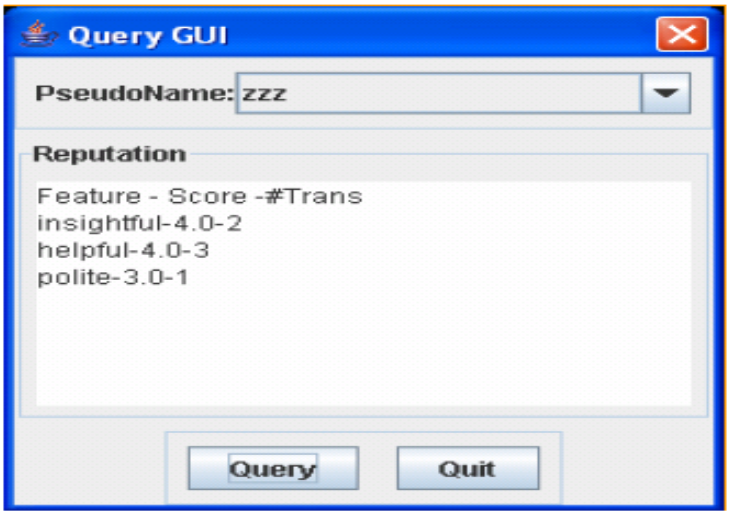


Figure 4.11: Screen shot of the result of reputation query for a pseudonym

quests a reputation transfer, it presents the registration number and the reputation digest (originally provided to it by the guarantor) to the guarantor, so the guarantor could authenticate its identity and retrieve its reputation. The guarantor then awaits consent (of reputation transfer) from another pseudonym, say *JerryTheSage* in the form of presenting its (i.e. *JerryTheSage's*) registration number and reputation digest. The guarantor transfers/merges *TomTheHelper's* reputation to *JerryTheSage* only when they appear to be a registered participant making a simultaneous request. Empirical tests successfully showed that the transferring aspect of the system works.

4.4 iHELP Discussion Scenario

The implemented ITMP and RT models in the form of privacy and reputation features helps iHelp discussants maintain different degrees (context appropriate and user-chosen) of privacy and trust at different contexts. My research has augmented the iHelp Discussion system so that it now implements a role and relationship-based identity management system for privacy and a reputation-management system for trust. This was achieved by completing the following tasks:

(i) Creation of contexts and roles

(ii) Creation of user-, context-, role-, and relationship- level identities

(iii) Allocating users to roles and facilitating switching across roles and contexts by the users (as they qualify)

(iv) Gathering ratings about postings from posting readers to calculate reputation of posters

(v) Assumption of Guarantor role to monitor activities, calculate reputation, and link historical data to its owner to make users accountable for their actions

Imagine that we are observing four discussants: Bob, Alice, Joe, and Jill as they build and maintain their multiple identities and reputation to manage their privacy and trust using privacy-augmented iHelp system.

> This term is not going well academically for Bob. He wants to share his frustration with and seek advice from someone who could be sympathetic to Bob and give good advice. Bob logs into an iHelp Discussion client using his student id (i.e., Bob123). The system displays a context-role identity hierarchy for Bob. In the hierarchy, there is a generic contexts: General Discussion with two sub-contexts **UnderGrad Discussions** and **Grad Discussions**. Under General Discussion, **all** and **devel** roles are listed.

Each context manifests some purposes for Bob's participation, and a list of roles under a given context states various capacities of Bob to participate in that context. Each context has a group identity for all the participants in that context and denoted by a pseudonym (e.g., *Discussion#* for General Discussion). A participant's context-level identity reveals their affiliation to a context. Likewise, each role also has a group identity for all the participants assuming that role and denoted by a pseudonym.

> Being sympathetic to others, Alice, a senior graduate student, wants to wear her compassionate mentor hat. Alice logs into an iHelp Discussion client using her student id (i.e., Alice321). While reading postings under the **General Discussion** context, she fixates on a posting from *Mr. Miserable*, who is overwhelmed by the course workloads. She clicks on

> the reply posting link to dispatch some advice to *Mr. Miserable*. The system presents a list of pseudonyms, representing her multiple partial identities appropriate to the **General Discussion** context, to choose from as a replier of that posting.

A discussant can have three types of pseudonyms to represent their various partial identities: user-level, category-level, and role-level. A user-level identity provides a discussant one identity for all different contexts. For example, *AliceTheDiscussant* pseudonym for a user-level identity allows a participant to maintain publicity across various contexts and sub-contexts. Both the category-level and role-level identities can be represented by a generic (or a group pseudonym) or a user-defined (or an individual pseudonym). A category- or role-level group identity makes a participant indistinguishable from other group members. A user-defined category- or role-level pseudonym allows a participant to be distinctive. A user-defined pseudonym embodies a relationship identity, since a discussant uses this pseudonym to present an identity to negotiate relationship with other discussant in a context.

> Since Alice wants to follow up on *Mr. Miserable*'s situation, she chooses to use her relationship (contextual, user-defined) pseudonym, *Ms. Mentor*. In response to his posting made using a category-level user-defined pseudonym, *Mr. Miserable*, Bob reads the advice of *Ms. Mentor*. Before seeking further advice or revealing any more details of his situation, Bob clicks on the poster pseudonym, *Ms. Mentor*, to invoke the reputation manger of the system. The reputation manager displays Alice's reputation as *Ms. Mentor* on three features: competence, benevolence, and integrity.

In generating posters' reputation, their true identities are kept separate from their behaviors. A poster is evaluated based on the quality of their postings. The quality of each posting is rated against the following matrices: insightful, well-written, informative, timely, constructive, and relevant. A rater may rate a posting against multiple matrices as appropriate on a 0 to 5 scale. For a user-level pseudonym, a participant is evaluated on all but the postings made under other user-level pseudonyms. A poster's competence is measured by their insightful, well-written, and informative

postings. A poster's benevolence towards another poster is measured by their making of relevant and constructive criticism towards another posting. The integrity of a poster is measured by timeliness of their reply or constructiveness of their postings. For individual reputation, a real number score in the range of 0-5 is used. For group reputation (i.e. reputation against a group identity), the rubrics of excellent, good, and average are used based on the score ranges to describe the overall performance of the group members.

> Bob is happy with the reputation of Alice in mentoring capacity and chooses to continue the mentor-mentee relationship for a while. Bob notices some new postings made under the sub-context **Rookie**, a context popular among freshman undergraduates. One such posting thread is on null pointer exceptions. As an avid programmer and active member of the software development support group, Bob is assigned a **devel** role. Due to lack of time commitment, Bob does not want to use his relationship identity to reply to one of the postings regarding "null pointer exception". Rather, he uses the pseudonym **devel#** presenting his affiliation to the developer group to reply to the posting.

Even though an actor is allowed to take cover of their group identity, they are made accountable for their actions. Any posting made by an actor under any group identity is also counted in calculation of reputation for their user-level pseudonyms. For group reputation (i.e. reputation against a group identity), the rubrics of excellent, good, and average are used based on the score ranges to describe the overall performance of the group members.

> Joe, a shy freshman in Computer Science, is experiencing null pointer exception in his java programming assignment. He has already spent long hours in this assignment and he could not fix the problem. He hears that most of his peers are already done. He feels embarrassment in seeking help using her distinctive identity. Joe takes cover in the *Undergrad#* group identity and seeks help by making a posting under the **UnderGrad Discussions** context. Jill, a PhD student who taught this course in last summer, enjoys helping students and she wants to be recognized for her problem solving acumen. Jill replies to Joe's (i.e., *Undergrad#*) posting using her user-level pseudonym *JillTheSage*.

Now Joe sees three replies for his posting: one is from devel (i.e. Bob), another is from *JillTheSage*(i.e. Jill), and the other is from *Discussion#* (i.e., Alice). Alice's answer to the question is more generic in nature since she does not know the exact problem. Joe also realizes that Alice comes to this context as an outsider (from the parent context). Alice's answer helps Joe understand various exceptions. Since Jill taught this class before, she knows the types of mistakes beginner programmers make to generate null pointer exceptions. *JillTheSage*'s answer helps Joe the most to pinpoint the problem. Joe rates *JillTheSage*'s (i.e. Jill) posting 5/5 on insightful metric and 5/5 on relevant metric. Bob's answer was more about writing good codes so that the exception like null pointer could easily be avoided. Initially Joe was frustrated with that answer, however, he went back to the posting later. In Joe's rating, devel scored low on relevance, but high on informative metric. The group identity of devel maintains good reputation for competence. In consequence, Bob's reputation score for competence has also increased; however, Bob's reputation score for benevolence has slightly decreased.

Bob is assigned a TA role for the context of **CMPT100** course. Bob wants to be personable and helpful to the students of this course. Therefore, he invokes system's identity (pseudonym) creation tool, Aliases. Bob is asked pick a pseudonym to embody the intended new identity and choose an Alias Type from the list of contexts Bob has access to and roles Bob could assume. Bob chooses the context **CMPT100** and pseudonym *CMPT100TA*. Bob starts to notice that students expect full detail answers to their questions from friendly helpful identity behind the pseudonym of *CMPT100TA*. Bob wants to help students become self-reliant and self-confident who should try their best to find a solution to problems with little or no help. Instead of giving answers to problems of the posters, Bob starts giving useful hints to help posters find answers by themselves. For that purpose, Bob uses the group identity *CMPT100#* and limits his use of *CMPT100TA* to posting where a higher level of authority is needed.

For reflective learning and exam preparation, Joe wants to read the postings he made in the past. Joe has made postings under various context, role, relationship, and user-level identity pseudonyms. However, on the Joe's views of the posting window, the system writes **(me)** next to the

poster's pseudonym for all the postings made by Joe regardless of the use various type of identities including the group identities. When Joe replies to any posting, the system lists all the pseudonyms for the identities appropriate for the context of the message being replied. Joe could use his *Discussions#* pseudonym from **General Discussions** context in its sub-context UnderGrad Discussions, but not vice-versa.

The potential identity imprisonment and digital forgiveness features of Role- and Relationship- based Identity Management (RRIM) could help enforce accountability through guarantor administered investigation and sanction. In this way, RRIM could potentially balance privacy with accountability.

A discussion moderator (e.g. TA) observes an act of flaming by a student named Rebel, which is discouraging others to participate. The moderator locks this identifier (i.e. Rebel) and thereby reports to the guarantor of this context (i.e. the instructor) about the questionable act. Upon investigation, the instructor may lock the Rebel identity for a period of time allowing this user to post only as Rebel no matter what context or role. This allows the marker to monitor Rebel very closely for any further act of bad conduct. As Rebel demonstrates integrity in the next two weeks of discussion, the instructor may unlock the Rebel identity and allow the participant to assume a new identity, if desired.

4.4.1 Discussion and Critique

In this iHelp implementation, the system helped users identify their counterparts and purposes of communication (tasks of application layer of the ITMP model). The system-offered context tree and role tag in a posting helped users understand context of communication (tasks of context layer of the ITMP model). The system played the role of a guarantor in calculating and presenting reputation of users (tasks of trust layer of the ITMP model). The system helped users creating their contextual partial identities (tasks of identity layer of the ITMP model). Finally the system allowed users to participate in a discussion using an appropriate partial identity from a list of their partial identities (tasks of presentation layer of the ITMP model). The implemented privacy and reputation features of iHelp Discussion provide participants

with better control over the flow (partners with whom information will be shared), boundary (restricts dissemination beyond an expected space - purpose/ partner), and persistence (span of time that disclosed information should be available to an information seeker) of their personal information. However, since the pseudo-identities and pseudonyms offered by the identity management solutions are not linkable, the complete assessment of reputation can easily be disrupted by switching and shedding of pseudonyms. The implemented RT model transfers/merges reputation across partial identities with the aid of a trusted guarantor. As a result, both ITMP and RT models are validated through their implementation.

The privacy solution provided by the role and relationship based identity management is two-fold: on one hand, the role-relationship initiation feature contributes to privacy by constructing contextual identity. On the other hand, forgetting of disclosed information is enforced by the following features: disavowing a relationship, temporal aspect of role and relationship, expiration of context, and disclosure/obligation management. The model also enforces accountability by holding an actor responsible for foul acting through guarantor administered investigation and sanction.

Due to the temporal dimension of role or relationship, any information released under a role or relationship ought to be virtually unusable for the counterpart when the respective role or relationship expires. Anytime, a participant fears a privacy threat in a relationship-based identity, the participant may abandon their respective relationship-based pseudonymous identity and take refuge in their role-based identity. The participant can negotiate a new relationship at any time and craft a new relationship-based identity. Even though a context-level identity provides a higher degree of anonymity, it is more desirable than full anonymity. A context-level identity reveals one's affiliation to a context. For example, CMPT280 is a follow-up course of CMPT270. The discussion forum for CMPT270 may be kept open for students, instructor, and TA of CMPT280 so that the students of CMPT280 can reflect on what they have learned and help the students of CMPT270. A context-level identity of someone from CMPT280 appropriately present them to students of

CMPT270, where as, an anonymous participant could be anyone in the courses or not.

In addition to the implementation of the RT model, the implementation of RRIM also addresses the issue of reputation earned on one partial identity in a context flowing over the other partial identities. It supports reputation merger - building reputation across multiple partial identities (aggregating reputation based on the performance under group identity). The implementation can help participants make an informed decision regarding what information to share with whom and to help control the persistence and boundary of disclosed information so that learners' privacy is not at risk even after disclosure of some personal information.

Chapter 5

Experimental Results and Analysis

Since Role- and Relationship-based Identity Management (RRIM) is an implemented instantiation of the generic Identity and Trust based Model for Privacy (ITMP), the effectiveness of the ITMP model is assessed through two studies on the effectiveness of RRIM in facilitating a privacy-enhanced discussion forum in the e-learning domain. The Reputation Transfer (RT) model, which is used in the trust layer of the ITMP model, is assessed in two ways: (a) in the assessment of RRIM, the embedded partial RT model is assessed, (b) the full implementation of the RT model is evaluated through simulation and by a human expert.

5.1 Role and Relationship-based Identity Management (instantiation of the ITMP)

The RRIM model was implemented as an extension to the existing iHelp Discussions tool, an online discussion forum in use at the University of Saskatchewan as part of iHelp e-learning system. The evaluation of the implemented RRIM features in offering privacy (through identity and trust management) is done in the following two user studies: (i) a pilot study and (ii) a larger-scale study. The studies were approved by the University of Saskatchewan Advisory Committee on Ethics in Behavioural Sciences Research (BSC# 2001-198).

The studies were designed and conducted to gauge the effectiveness of RRIM in providing privacy through identity and trust management. In the study, answers to the following question are sought through analyzing usage data and user interview

data: how effectively does the implemented system facilitate context dependent selective disclosure of identity? In finding answers to this broader question, I generate the following more specific questions, which are addressed through analyzing usage data and post-use survey (see Appendices C and D):

Q1. To what extent does context awareness help users to maintain privacy?

Q2. To what extent does the system facilitate information sharing based on trust?

Q3. How effectively does the system promote context awareness?

Q4. How easy (or burdensome) are the tasks of creating and maintaining multiple contextual identities?

Q5. How effectively does the system inhibit information linkage attacks?

Q6. How well does the system promote personal autonomy and freedom (i.e. are the participants more authentic and less guarded)?

Q7. How safely does the system allow users to express their seminal and inchoate ideas?

5.1.1 Pilot Study

Methodology

In the pilot study, the system was initialized to generate several different discussion contexts. For each context, the system allocated one or more desired roles to each discussant. Additionally, the system offered three types of pseudonyms to each participants: a. a user-level pseudonym type to represent a discussant across contexts, b. a context-level group identity type for each context, representing the group of discussants participating in a given context, and c. a role-level group identity type for each role within a context, representing the group of discussants, participating in a given role in a given context. The system logged activities of the discussants which were analyzed to help in answering the above proposed questions.

Seven different topics (contexts) of discussion were chosen, representing the following issues: a. Same-sex Marriage, b. Abortion, c. Tibet Issues, d. Mission in Afghanistan, e. Collaboration vs. Plagiarism, f. Schools Kill Creativity, and g. Net Neutrality. Out of these seven issues, the first five are quite controversial, and the last two of them are less controversial or more agreeable in nature for the students while discussing with their peers. I suggested various roles to our participants to choose from to present their perspectives on different issues. Here are the suggested roles for the discussants of different issues.

- Same-sex Marriage: Proponent, Opponent, and Gay/Lesbian
- Abortion: Mother, Doctor, Religious Leader, Proponent, and Opponent
- Tibet Issues: Chinese Government, Tibetan, and Citizen of the World
- Canadian Mission in Afghanistan: Proponent, Opponent, Liberal, Conservative, and Afghan Govt.
- Collaboration vs. Plagiarism: Professor, Student, Collaborator, and Plagiarist
- Schools Kill Creativity: Student, School Administrator, Professor, Proponent, and Opponent
- Net Neutrality: Proponent and Opponent

I chose these rather controversial issues, because providing free speech while protecting one's privacy seems to be important. While discussing these issues, many people fear being embarrassed, looking foolish, or not being accepted. In recruiting participants, we have heard similar concerns from the individuals whom we approached for this study. One of our contentions is that role- and relationship-based identity management effectively supports self-reflection types of activities, one of the reasons why privacy is so desirable [Westin, 1967]. Some of the participants chose more than one, sometimes even quite opposite, roles on a given issue substantiating

our contention. I have also chosen two less controversial (or neutral) issues to compare participants' uses and experiments of identities and use of RRIM in catering to the need of different amounts of privacy at different contexts.

Results

In this study, five (volunteer) participants used our system for over a two week period, making 112 postings in seven different contexts (categories). The participants were Computer Science graduate students who were trained to use the system in a one-to-one session. Four of the participants were male while one was female. At the end of the study, each participant received a $20 honorarium. To encourage participation, email reminders were sent routinely. The usage activities (e.g. posting, querying fellow participants' reputation, etc.) of participants were logged to find the use of various key features of the system. Then a post-use survey was conducted to gather the participants' assessment of the system and to capture their attitudes and preferences towards privacy and trust. A 5-point (level of agreement) and 4-point (level of frequency) Likert scale together with text comment/input were used to collect participants' assessment/attitude data from the survey.

The average number of postings made using the three different identity types are the followings: user-level = 1.17 per participant, role-level = 10.5 per participant, and context-level = 7 per participant. The participants rarely used their user-level public identity. They preferred role-level identity over context-level identity. From usage data, we see that the participants checked each others' reputation 67 times. Combining the survey data with the usage data, we see that the participants, who care about reputation (-based trust) more, paid more attention to a poster with a good reputation, and therefore, queried others' reputation more. Interestingly, the participants, who did not care about others' reputation, still routinely inspected (cared about) their own reputation (Q2).

The participants could not correctly guess the number of different actual people who participated in the discussion (Q5). All the participants reported that they could rarely identify which postings belonged to which actual users. Operationalizing

context with respect to purpose and role is justifiable by survey results: 80% of the surveyed reported that taking on a role helped them reveal information selectively in a communication episode (Q1); 80% reported that the system helped them to keep in mind the purpose of a communication episode. Furthermore, since 80% of the participants reported that the system helped them create context-sensitive identities, we could say that context is well represented in the system.

All the participants have reported that the system offered them satisfactory (20% strong agreement and 80% agreement) level of privacy. In Table 5.2, we see that the users were not only satisfied with the system's performance, but also their abilities to maintain privacy while sharing their views. Table 5.1 reports participant's various level of desire for privacy. In Table 5.1, we see that 80% have experimented with their identity (by playing more than one role and making contrary posting using both role-level and context-level identities). All of them have intentionally made provocative postings.

Table 5.1: Users' desire for privacy

item	agree	undecided	disagree
more authentic (Q6) in posting because of RRIM's privacy features	60%	20%	20%
experiment with identity because of RRIM's privacy features	80%		20%
more direct in terms of language because of RRIM's privacy features	40%	40%	20%
less guarded (Q6) in communication because of RRIM's privacy features	60%	20%	20%
experience emotional release because of RRIM's privacy features	20%	80%	
intentionally provocative because of RRIM's privacy features	100%		

5.1.2 Larger-scale Study

Methodology

In the larger-scale study, the system was used to support online course discussion in a six credit intensive six-week undergraduate course on Introduction to Sociology (see Appendix A). The study was done in 2 phases: (1) In the first three week

Table 5.2: User satisfaction with the system

item	very satisfied	satisfied	neutral
privacy-protection offered by system	20%	80%	
own performance (maintain privacy while sharing views)	40%	60%	
control over identity choice	20%	80%	
control over disclosure of identity	20%	80%	
help in disclosing information (about self and beliefs) safely (Q7)	60%	40%	
awareness of identity provided by system (Q3)	20%	80%	
awareness of activity (postings) provided by system (Q3)	80%	20%	
easy-to-use system (Q4)	40%	40%	20%
easy-to-learn system (Q4)	60%	40%	

period, the class made 173 postings using the original version of iHelp Discussion (without RRIM), and (2) In the next three week period, they made 302 postings using a version of iHelp Discussion with RRIM and RT features. In each phase, the participants (students and the instructor) discussed topics under eleven contexts, each addressing eleven different social and behavioral questions. Prior to each phase of the study, users were trained to use the system. At the end of the second phase, 25 participants of the study took a post-use online survey to share their use experience and their attitude towards privacy and trust.

The participants discussed answers to 22 questions, 11 questions in each phase, using their personal experience and sociological knowledge. These questions are chosen by the instructor of the course as per the course objectives. In the first phase, they used the original iHelp, which required them to use their public identities (i.e. first initial followed by last name) to post a new message or to reply to a post. For the phase 2, discussants used the augmented version of iHelp, which allowed them to create multiple role- and relationship-level identities, provided awareness support of contexts and identities, and enabled them to rate others and query others' as well as their own identity-specific reputation. The following eight roles were suggested (and offered in the system) for the discussants (to take on) to shed perspectives of respective roles on different contexts:

- Devil's Advocate

- Right-wing Conservative
- Environmentalist/ Activist
- Sexist
- Apathetic
- Deep thinker/Intellectual
- Luddite
- Miss Congeniality

In the phase 2, in addition to the public identity, the system offered three types of pseudonyms to each participant: (i) a user-level pseudonym type to represent a discussant across contexts, (ii) a role-level group identity type for each role within a context, representing the group of discussants, participating in a given role in a given context, and (iii) a role-level individual identity type for each role within a context, representing an individual participating in a given role in a given context. Since, unlike the pilot study, there is no hierarchical relationship among contexts presented in the phase 2, the context-level pseudonym is omitted in this larger-scale study. Like the pilot study, the system logged activities of the discussants to be analyzed for answering the questions presented at the beginning of the Section 5.1.

Results

After the privacy-enhanced version of iHelp was introduced, participants made 4.40% of their postings anonymously, 35.59% of postings using their public identities, and 58.98% of postings using role-based identities. With in role-based identities, 22.03% of postings are made using system-provided group-level identities (e.g. Devil# for Devil's Advocate role), where as 36.95% of postings are made using individual role-based identities (relationship-level identities). 1.01% postings are made using user-level identities. A significant use of role-based and both group-level and relationship-level identities underlines the significance of role- and relationship-based identity

management and appropriateness of operationalizing context in terms of roles and relationships.

Unlike the participants of the post-use survey of the pilot study, the participants of this large-scale study had a chance to compare the original version of iHelp with the augmented version of iHelp. The following item from the survey is an example where the survey-takers are asked to compare their use experience of the two versions:

> The system enabled me to act more candidly using my partial identities (in version 2) than I would have done using a single "real identity" (in version 1)

On this item 52% of the survey takers agreed, while 4% of them disagreed. The entire post-use survey appears in Appendix D. Table 5.3 reports survey responses as percentages (relative frequencies) of agreement and disagreement to different likert items.

An analysis of usage data indicates a 75% increase in participation from the original version of iHelp. Table 5.4 compares participations in original iHelp version with participation in privacy- and trust-augmented iHelp version. As we know that all learners do not participate equally in a discussion, we see a high standard deviation in participation for both the original and the privacy-augmented versions of iHelp. Moreover, privacy does not equally matter to everybody. Those who cared for privacy and felt safe participated much more than others. Figure 5.1 (x-axis = posters from least to most, y-axis = number of postings) shows a significant over all participation increase in the privacy-augmented version of iHelp from the original iHelp. A paired t-test indicates a significant increase in participation in privacy-augmented iHelp from the original iHelp at t= -2.1136 , p=.0208. Anecdotal accounts of the students and observations from the instructor also suggest that the privacy and trust features have increased their participations. The followings are some remarks from the students and the course instructor.

> "We are more comfortable participating in the 2nd version (augmented) than participating in the 1st (original) version."

> The course instructor commented, "The quality of participation has improved in the 2nd version. More open, more fun."

Table 5.3: User survey response(larger-scale study)

item	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Satisfied with Overall Privacy	36%	40%	24%	0%	0%
In-obtrusive	36%	12%	44%	0%	8%
Satisfied with Privacy-preserving Info Sharing	44%	32%	24%	0%	0%
Felt in Control of Identity Choices	36%	40%	20%	4%	0%
Satisfied with Identity Disclosure	36%	24%	36%	4%	0%
System Helped Identifying Trustworthy	12%	16%	60%	4%	8%
Act More Candidly Using Partial Identities	16%	36%	44%	4%	0%
Valued Postings Based on Poster's Reputation	20%	16%	32%	8%	24%
Found the System easy-to-use	40%	20%	28%	8%	4%
Found the System easy-to-learn	36%	16%	36%	8%	4%
System Helped Me Maintain Privacy	32%	40%	20%	8%	0%
System Helped Me Identify Trustworthy Posting	16%	24%	52%	0%	8%
System Facilitates Trust	24%	36%	40%	0%	0%
Helped Me Communicate Appropriately in Context	36%	32%	32%	0%	0%
Helped Me to Safely Disclose Info	40%	28%	32%	0%	0%
Helped Me to be Aware of Context	24%	28%	48%	0%	0%
Replied More Often to Posters with Good Reputation	12%	16%	40%	16%	16%
Paid More Attention to Posters with Good Reputation	24%	12%	36%	16%	12%
Rated Postings with a Purpose to Reward/Discipline	12%	16%	40%	16%	16%
More Open when Replying to Posters with Good Reputation	4%	24%	48%	12%	12%
Spend More Time on Quality Postings	24%	32%	28%	16%	0%
Helped Me to be Aware of my Assumed Identity	24%	28%	44%	4%	0%
Able to Separate my Postings from Others	32%	32%	28%	0%	8%
Aware of Expected Behavior of Assumed Identity	36%	28%	24%	8%	4%
Able to Link Postings	8%	28%	36%	16%	12%
More Authentic in Privacy-augmented iHelp	28%	16%	44%	12%	0%
More Direct in Privacy-augmented iHelp	32%	28%	32%	8%	0%
Used Group Identity to Rant	24%	20%	40%	8%	8%
Intentionally Provocative because of Identity Choices	28%	20%	44%	4%	4%

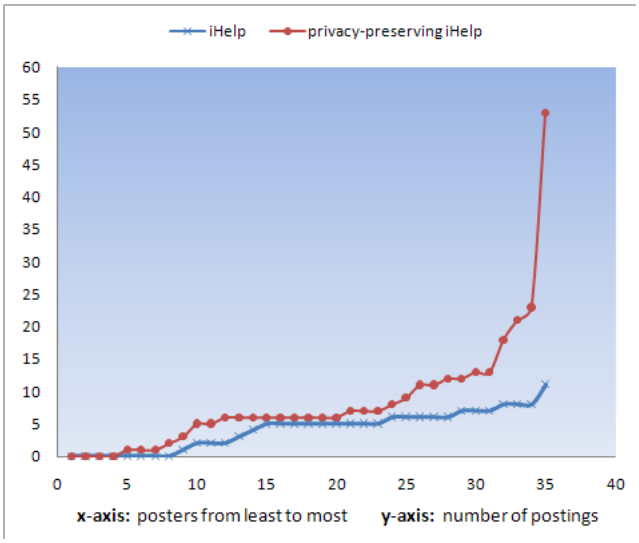


Figure 5.1: Participation comparison graph(larger-scale study)

"Very good idea, allows for discussion outside of class. Hope to see it utilized in other classes."

"I found that I had to read the same postings more than once because there were different ways (different identity choices) to reply to the questions (comments)"

Table 5.4: Participation comparison(larger-scale study)

	mean posting/participant	σ
Original iHelp	4.75	4.68
Privacy-augmented iHelp	8.44	9.46
Overall	6.6	

The usage data reveals that every participant has received reputation ratings on their posts and that 43% of the participants have checked their own or others' reputation. On an average, each participant received 12.5 ratings. 31% of the participants consulted self reputation.

The survey indicates that those who perceived that their privacy was maintained were more direct and authentic in their communication. Some of the participants who were satisfied with their privacy also experienced emotional release using their multiple partial identities. Further analyses of the survey data of Table 5.3 confirm our hypotheses about the relationships between privacy and each of context, identity, and trust.

Hypothesis 1: *Understanding and awareness of contexts contribute to privacy-preserving information sharing.*

To test hypothesis 1, the survey takers' levels of privacy satisfaction are considered dependent variables. This is compared against their agreement in the following two independent variables: (1) the system helped them communicate appropriately in a context, and (2) the system helped them to be aware of the context of a communicative episode. Thus I tried to predict levels of privacy satisfaction from understanding and awareness of context. We see in Table 5.5 that the understanding and awareness of context contribute to privacy satisfaction. The impacts of appropriate contextual communication and context awareness on privacy satisfaction are statistically significant (t=2.6 and t=2.5 respectively). Those who experience appropriate contextual communication also are satisfied with their privacy (β=.48, p=.016). Those who have greater awareness of context also are more satisfied with privacy (β=.47, p=.019). The R-square indicates that 54% of the variation in the users' level of privacy satisfaction is explained by the set of independent variables representing their understanding and awareness of context. Therefore, we can conclude that results from multiple regression in Table 5.5 confirm our hypothesis that the system provides adequate understanding and awareness of context contributing to privacy-preserving information sharing.

Table 5.5: Context contributes to privacy (larger-scale study)

Dependent	Independent	Coefficient (β)	R-square	t	p (acceptable < .05)
Privacy Satisfaction	Appropriate Contextual Communication	.48	.54	2.6	.016
	Awareness of Context	.47		2.52	.019

Hypothesis 2: *Identity management (awareness and control over identity) contributes to privacy-preserving information sharing.*

To test hypothesis 2, the survey takers' levels of privacy satisfaction are considered dependent variables. This is compared against their agreement in the following three independent variables: (1) they felt in control of their identity choices, (2) they were

satisfied with the way the system enabled them to manage how they disclosed their identities, and (3) the system enabled them to act more candidly using their partial identities. Thus I tried to predict levels of privacy satisfaction from their satisfaction in the system's offered identity management features. We see in Table 5.6 that awareness and control over identity contribute to privacy satisfaction.

Table 5.6: IM contributes to privacy (larger-scale study)

Dependent	Independent	Coefficient	R-square	t	p (acceptable < .05)
Privacy Satisfaction	Control of Identity Choices	.69	.67	3.2	.004
	Manage Disclosure of Identity	.15		.81	.43
	Act candidly using partial identity	.23		1.6	.12

The control over identity choices has statistically significant impact on privacy satisfaction. Those who experience control of identity choices also are very satisfied with their privacy (β=.69, p=.004). Those who act candidly using partial identity also are satisfied with their privacy (β=.23, p=.12). However, those who managed disclosure of identity are not very significantly satisfied with privacy (β=.15, p=.43). The R-square indicates that 67% of the variation in the users' level of privacy satisfaction is explained by the set of independent variables representing their satisfaction in identity management features.

Therefore, we can conclude that results from multiple regression in Table 5.6 confirm our hypothesis that the system provides adequate identity management support contributing to privacy-preserving information sharing.

Hypothesis 3: *Trust can be used to manage privacy.*

To test observation-3, the survey takers' levels of privacy satisfaction are considered dependent variables. This is compared against their agreement in the following two independent variables: (1) the system facilitated trust, and (2) they were willing to be more open when they reply to posting from a person with a good reputation. Thus I tried to predict levels of privacy satisfaction from their satisfaction in the

system's offered trust and their willingness to use trust to manage privacy.

Table 5.7: Trust contributes to privacy (larger-scale study)

Dependent	Independent	Coefficient	R-square	t	p (acceptable < .05)
Privacy Satisfaction	More open to trustworthy	.1	.25	.34	.73
	System facilitates trust	.47		1.29	.21

The multiple regression results in Table 5.7 show that the independent variables (two of the reputation statements) do not have significant impacts on users' privacy satisfaction (p=.73 and p=.21). Therefore I cannot confirm my initial observation that the system supports proper trust management contributing to privacy-preserving information sharing. However, I realize that the need for reputation or trust in the study is not as critical as it is in an online setting where there is no bodily presence to act as a trust guarantor. Since the participants of this study are classmates, they are already involved in trust relationships. They would have felt the need of trust and acted differently, had they acted in online where there is no physical interaction.

Analyzing survey takers' desire for privacy, we see that 32% strongly agree and 28% agree that they were more direct in expressing their views in privacy-augmented iHelp than they were in original iHelp. 28% strongly agree and 16% agree that they were more authentic to other participants in privacy-augmented iHelp than they were in original iHelp. 24% strongly agree and 20% agree that they used group identity when they wanted to rant. 28% strongly agree and 20% agree that they were intentionally provocative because of identity choices offered by the privacy-augmented iHelp system.

5.2 Reputation Transfer (RT) Model

This section reports on a study validating the implementation of the RT model. The study was designed to see whether the system facilitates reputation-based trust

while preserving privacy by making secure reputation transfer/merge across multiple pseudonyms.

5.2.1 Methodology

For the above purpose, the system was initialized to generate multiple instances of four types of events (reputation evaluation request, reputation transfer request, reputation merge request, and null requests) in some random order for n pseudonyms representing m actors. At multiple time steps during the simulation, the system (the component representing the guarantor) was queried for the latest reputation of each of the $n*m$ registered pseudonyms and the query results are logged. A version of this simulation was run for $n = 4$, $m = 2$, and reputation update actions were logged accordingly. These logs (in Figure 5.2) were then provided to a security attack-defense expert to attempt to deduce types of events might have occurred based on an analysis of the reputation score patterns over various time steps. The expert was also asked to see whether he could distinguish among or determine instances of reputation transfer, reputation merge, and normal updates of reputation ratings.

5.2.2 Results

Table 5.8 shows the simulation performed 3 transfers and 7 merges of reputations across four pseudonyms of two actors. Although the data set was relatively small, the expert could not make any definitive conclusions that would identify which pseudonyms corresponded to the same actor. Our expert suspected that four mergers or transfers of reputation occurred.

The one merger hypothesis in which the expert was most confident was totally incorrect. Two of our expert's suspected mergers or transfers actually did correspond to real mergers or transfers, but the expert entirely missed eight of the merger/transfer events. Our expert correctly had a suspicion that one transfer and one merger (of the ten) had occurred, but he could not be sure. Out of these 2 correct hypotheses, the expert could not confirm conclusively about any of the mergers or transfers.

We could say that these correct guesses are no more than random luck. With an increase in the number of actors or pseudonyms, it becomes even harder to guess about any reputation transfer or merge. Therefore, we could say that our system supports reputation transfer with privacy preservation.

Table 5.8: Reputation pattern analysis

	Total	Correct Guess	False Positive	Undecided
Transfer	3	1(unsure)	1	1
Merge	7	1	1	5

5.3 Conclusion

In this chapter, the verification and validation experiments of the Identity- and Trust-based Model for Privacy (ITMP) and the Reputation Transfer (RT) model are reported. An implementation of the Role- and Relationship-based Identity Management (an instantiation of ITMP) together with some features of the RT model in the discussion tool of the iHelp e-learning environment were studied. With encouraging results from a small pilot study with 5 graduate students, a large-scale study was conducted with 25 students (35 used the system) in a sociology class. In the larger-scale study, the functionalities and usability of the models were retested. With consistent and reliable evidence, the survey and usage data indicate that the system offered users a satisfactory-level of privacy while allowing learners to exchange their views (sharing information).

Analyses of survey data confirm the following two hypotheses : (a) Understanding and awareness of context offered by privacy-augmented iHelp contribute to privacy-preserving information sharing (b) Identity management (awareness and control over identity) offered by privacy-augmented iHelp contributes to privacy-preserving information sharing. However, we cannot confirm from this study the assumption that trust and reputation can be used to manage privacy for the following two reasons: (i) less than half of the participants used trust and reputation features of the system, and (ii) since the participants were classmates in a fairly small face-to-face class,

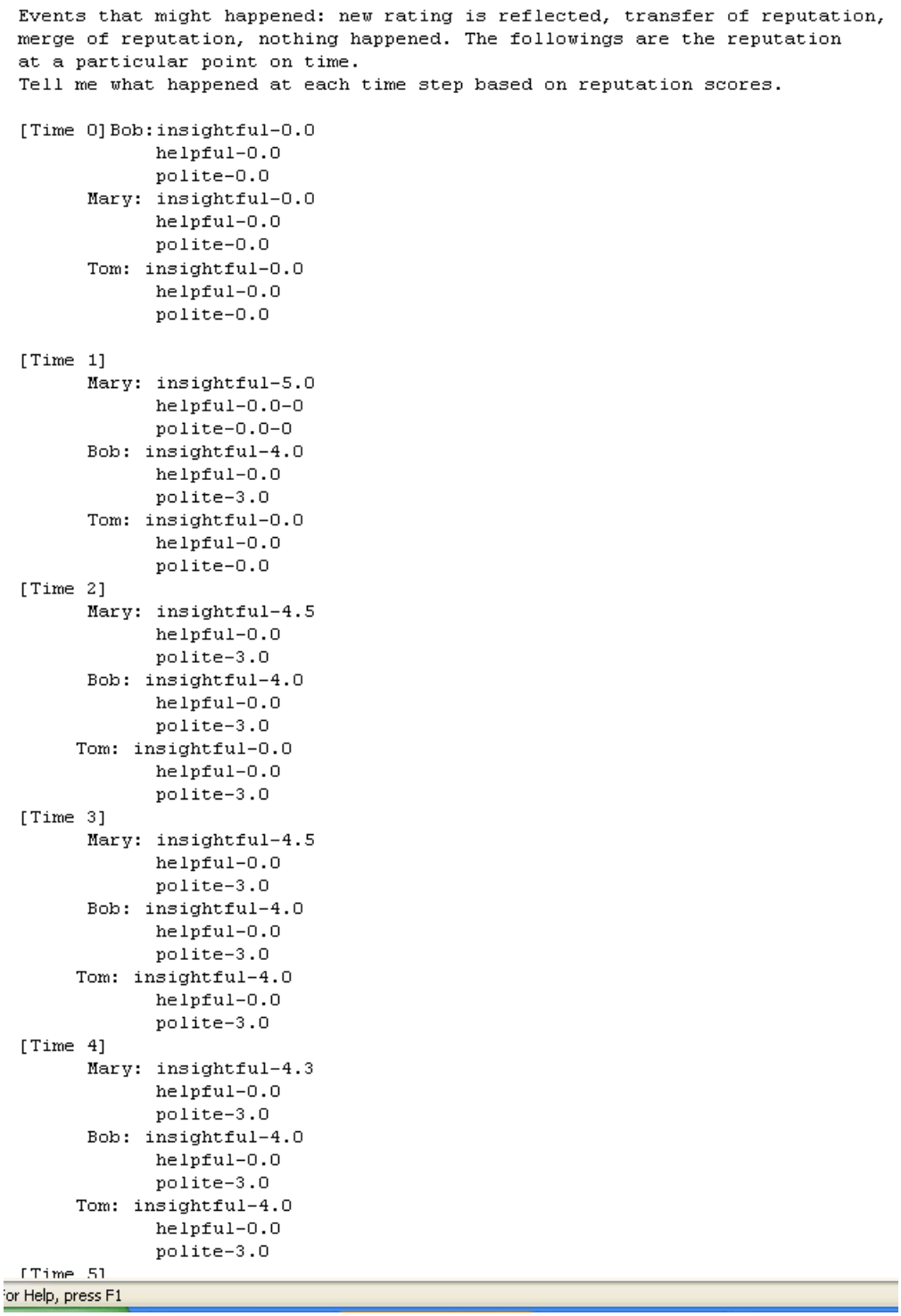


Figure 5.2: Subset of reputation transcript log for three of the eight pseudonyms

they were already involved in a trust relationship, and majority of them had no expectation of trust from the system. However, it is observed that those who cared about trust measures used the trust and reputation features of the system more extensively. The survey data also indicate that a significant portion of the participants were more direct and authentic in expressing their views in privacy-augmented version of iHelp than the original version. Overall, the participants reported enjoying the privacy-augmented version more than the original version of iHelp.

A stand-alone implementation of the RT model was also tested through simulation and human-expert testing. The test results show that the implemented system performs reputation transfer/merger in a secure and unobservable way in addition to generating reputation from the longitudinal study of behaviors. Therefore, the system supports assessment of reputation in a privacy-preserving manner.

The findings of the two user studies and simulation-human-expert testing of reputation transfer have been able to confirm answers to the two research questions this thesis aimed to address. In answer to research question1, context, identity, and trust are identified as three key factors to be considered in building a solution to privacy. In answer to research question2, a generic model has been constructed using three key factors of context, identity, and trust. An instantiation of that generic model was implemented as an augmentation to iHelp Discussion system, which was demonstrated to work effectively in two user studies. The participants of the studies found privacy-augmented iHelp as a privacy-preserving information sharing tool. Specifically, statistical analysis of usage and survey data confirm the role of context and identity in preserving privacy.

Despite the inability of the studies to confirm the role of trust in preserving privacy, we see a significant use of trust features by some of the participants and their willingness to use trust to manage privacy. In order to build privacy-preserving information sharing paradigm, privacy-preserving reputation assessment has to be supported. The simulation and human-expert based testing of the proposed reputation transfer model confirm the effectiveness of privacy-preserving reputation assessment.

Chapter 6

Conclusions

This chapter summarizes the research work presented in this thesis. This chapter also reports limitations of this research together with contributions made by this research. Many avenues for future work stem from this thesis, and are also presented in this chapter.

6.1 Summary

In this thesis, the issues of and the existing solutions to privacy in the online world are investigated through a comprehensive multi-disciplinary literature review. In addressing the findings of the literature review, this thesis operationalizes the notion of privacy (in the online world) and constructs computational models as a solution to privacy. The proposed models are applied in the particular online domain of e-learning. These models are verified and validated through an implementation followed by two user studies (a pilot and a larger-scale study). Results from these studies confirm that the models deliver their anticipated functionalities in a usable manner to their users.

Privacy is a subjective and contextual notion. Privacy is subjective since it is preserved when an individual's expectation of others to use their personal information in their anticipated manner is fulfilled. It is contextual since an individual's expectation for privacy varies (from "absolute privacy" or anonymity to "no privacy" or publicity) from one context to another. This thesis views that an individual's expectation of privacy can be fulfilled by enabling them to control various aspects of their personal information. Stemming from that view, a working definition of privacy is

provided: An individual's privacy is their ability to control the flow, boundary, and persistence of their personal information.

To equip users with a mean to control the flow, boundary, and persistence of their personal information (and thereby, obtain their desired privacy), an identity and trust based model for privacy (ITMP) is proposed. The key components of this model are context, identity, and trust. The context of an information sharing episode is captured through identifying purpose, role, and relationship. An identity consists of a dataset representing attributes and reputation of an entity in a given context. Trust is measured by reputation earned in a given context along dimensions of competence, benevolence, and integrity. This model delivers privacy by contextualizing (associating each identity with a context) and separating identity from behavior and helping users make a trust-based decision regarding sharing information.

6.2 Limitations

In this thesis, the generic ITMP model is implemented and validated in the e-learning domain. The generality of results can be achieved only through further validation of ITMP in other online domains. Despite this limitation, this research achieves my initial research goals and answers the initial research questions by comprehending issues, constructing models, implementing the models in a particular domain, and validating models through user studies.

The generic ITMP model and its instantiation (RRIM) have been shown help users make an informed and judicious privacy decision and empower them to hold control over their disclosed information. However, this thesis assumes that users act rationally and according to their expectation of privacy. Otherwise, the proposed privacy solutions will not be able to ensure privacy. For example, we assume the user will not openly present identifying data such as their real name or permanent address that may allow their partial identities to be linked.

The ITMP model assumes that its application layer will be able to identify the role of and relationship with the counterpart and purpose of communication in a

communication episode. This assumption may not work well in an open, diverse, and distant community or across communities. However, with the use of authentication and identification security technologies (e.g. digital signature) and effective communication between application layers, this model can perform as expected.

The trust layer of this model requires a trusted public actor, namely guarantor, for the complete assessment of reputation across partial identities (performing transfer and merge of reputation). Even though the RT model offers provably unobservable and secure reputation aggregation across partial identities, an individual may conceal a partial identity or some identities to the guarantor and the community. An undisclosed identity may be irrelevant to a user's persona within the community, or the user may choose to play differently than that of their hidden identity within the community. In any case, this does not affect the model in any way. However, one may initially build good reputation to earn the confidence of others to collect their personal information and later breach their privacy expectation. To minimize the impact of this problem, a generic notion of information expiration is introduced by means of disassociation of identity from disclosed information.

The research presented in this thesis does not intend to build a specific tool for privacy, or personalization, but rather, it provides a generic model that can be used to build tools for privacy-preserving information sharing, which in turn can facilitate personalization. It is a generic model, and therefore, like any generic model, it has to be interpreted for a specific domain. This thesis identifies many, but does not study or address all of the issues that ensue privacy concerns. For example, lack of awareness cues or conflicts of information rights among multiple parties complicate the privacy problems. However, pursuing all the interesting issues is beyond the scope of this work.

No matter what laws are passed, and how good the security measures might become, they will never be enough to ensure adequate privacy. We also need to develop and act according to some shared ethical values and enhance privacy and trust through responsible behaviour. We need to protect user data from misuse by implementing policies, standards, and fair information practices. All the parties

who have a stake in the Internet infrastructure needed to work together to make appropriate policy and technology that would provide us with personal space, help us build a web of trust, and thereby exploit the full potential of the Internet.

6.3 Lessons Learned

6.3.1 Comments on the Experimental Results

The experimental results are supportive of our key hypotheses and assumptions, especially in confirming that understanding and awareness of context and proper management of contextual partial identities help users maintain their desired amount of privacy. The analyses of usage data and user survey data from both the pilot and larger-scale studies show that the system provides users with control over the choices and disclosures of their identities and awareness of their identities and behaviors. Even though reputation was not as important in these experimental settings as it is in finding good helper or trustworthy friends in the online world, we see that some participants made use of reputation in paying attention to postings, in trusting a posting, and in rewarding or disciplining posters.

Due to the public nature of discussion in our studies, we could not check in these experimental settings whether an individual is more open to another individual with higher reputation. However the 80% of the participants of our pilot study reported that they maintained integrity of their identity for good reputation. Even though we have seen different level of desires for privacy, we have seen unanimous agreement from both the usage and survey data that our system fulfills the need of users' privacy.

6.3.2 Issues and Challenges in the Design of a Solution to Privacy

- Since privacy is a subjective notion, any solution to privacy has to be user-centric. A user's input for their desired amount of privacy (absolute privacy

to publicity) in a communication episode has to be taken into account.

- The expectation of privacy is influenced by other expectations and needs such as security, trust, and personalization. In providing a solution to privacy, these expectations and needs have to be accommodated. Therefore, a holistic approach to privacy is most effective.

- Privacy without accountability is counter-productive. A solution to privacy is more acceptable when the solution ensures accountability of user behaviour.

Evaluating the effectiveness of a privacy solution is quite a challenge. It depends on the privacy seeker's expectation of privacy in a context and the fluidity of their expectation over time or across contexts. Moreover, one individual's expectation is quite different from another. Even a subjective analysis in the form of a user-study cannot entirely judge the effectiveness of a privacy solution since all the participants in a study may not experience all the scenarios, in which privacy matters to them. This thesis tries to address this challenge (in both the user studies) by providing communication episodes that are rather controversial in nature, and therefore, where privacy becomes more important.

6.4 Contributions

Security is one important factor that contributes to privacy by means of access control and authentication. The research done for this thesis has explored other important but not as well recognized factors that support privacy, which include context, trust, and identity. This thesis introduces the notion of privacy-preserving information sharing by presenting an appropriate partial identity to a partner using trust and analyzing communicative contexts. Trust is portrayed as reputation of the partner and justification of the purpose of information disclosure. Context is described in terms of roles and relationships between information seeking and information giving partners.

To build a user-centric computational model for privacy, a notion of privacy from users' perspectives is required. This thesis has introduced a user-centric notion of privacy for information sharing situations: privacy is characterized as users' intended level of control over flow, boundary, and persistence of their disclosed personal information. A 5-layer privacy model, consisting of application, context, trust, identity, and presentation layers is outlined in order to achieve privacy objectives. In this model, the control over flow, boundary, and persistence is implemented in the following ways: restricting secondary use allows its owner to have control over the boundary of their information; information expiration allows its owner to have control over the persistence of their information; informed disclosure decisions help its owner to control over the flow of their information. Developing a model to enforce the mandatory forgetting of information seems to be very difficult. In that vein, the proposed ITMP model enforces information expiration by making old information irrelevant. Ultimately, I hope this thesis work will contribute to future research in privacy and related areas, improving and enriching various domains like e-learning, where personalization and privacy are both important. In summary, this thesis makes the following contributions to the research on privacy, trust, identity management, personalization, and e-learning:

- This research is expected to contribute a significant body of theoretical and analytical knowledge concerning privacy, trust, identity, and communicative contexts in the online world. This knowledge forms the basis of the answers to research questions #1 and #2 that guide this research.

- This research provides holistic analysis and discourse about privacy focusing in e-learning and other applications (research question #1). The user-centric notion of privacy significantly affects the design of a privacy solution. I feel this contribution has the potential to significantly impact the way privacy enhancing tools (PETs) are designed, analyzed, and evaluated.

- The ITMP model provides guidance for privacy solution designers. This model provides control to an individual over the flow, boundary, and persistence of

their information. By building a more general framework, I expect to enable the application of privacy-preserving communication and collaboration (research question #2) to a broader variety of fields.

- A mechanism to attach and remove reputation to/from a pseudonymous identity can help facilitate trust without the loss of privacy. Though pseudonymity supports reputation marking (attached to each pseudonym) based on the observed actions, it does not provide a mechanism for reputation transfer. This thesis also presents a reputation transfer model as part of the ITMP model for privacy.

- This thesis presents an instantiation of the generic ITMP model in the e-learning domain and an implementation to prove or verify the model.

- This thesis also presents results of a pilot and a larger-scale study with human subjects that help validate the ITMP model.

- This thesis identifies and addresses a generic limitation of identity management that it hinders complete assessment of reputation. In this vein, this thesis presents the reputation transfer model for reputation aggregation (transfer/ merge) across the partial identities of a person.

- This thesis presents a mechanism for privacy-preserving personalization by means of the use of sessional tokens.

6.5 Potential Impact

This thesis could contribute to improving the design of Cardspace, Microsoft's identity management-based solution to privacy. This thesis views reputation as a key part of identity. Implementing the RT model in Cardspace, reputation could be assessed across cards. Attaching reputation to self-asserted cards may increase their credibility and acceptability. One of the limitations of Cardspace is that the system does not help users choose an appropriate identity card for a given context.

Implementing the context layer of the ITMP model in Cardspace may help users understand a context and choose an appropriate card for a given context.

In Cardspace, trust is defined as the willingness of a person to believe the claims asserted by certain others (for example, Verisign marking on a website). But users need to know whether the site can be trusted to share certain information. Implementing the context layer of the ITMP model in Cardspace may help users make a trust-based privacy decision. Moreover, Cardspace does not address improper retention and use of users' information. My generic notion of information expiration by disassociating identity from disclosed information may help Cardspace address improper use and retention of users' information.

6.6 Future Work

During the course of comprehensive survey of works to date on privacy, I have identified many promising areas of exploration that apply to privacy-preserving information sharing. In this section, I detail several interesting problems, in which I am confident that I or others may obtain results in future research.

- Conflict (of info right) Resolution: "Privacy is an interaction, in which the information rights of different parties collide" [Noam, 1997]. In various contexts, information of individuals propagates through various partners and channels, convoluting the issues of ownership over information. Moreover, a piece of information may be claimed by more than one party and they may differ in their requirements for privacy. For example, Joe and Mary may have different preferences in sharing their collaborated ideas or their conversation to others. Addressing this issue would require identifying and propagating ownership meta-information with the propagation of information. In case of multiple owners, the owners' preferences and requirements for privacy need to be aggregated and factored into a disclosure decision.

- Awareness Cues: In a face-to-face communication, one can look in the eye of the interlocutor and search for tacit signs of truthfulness or falsehood [Feenberg, 1989].

On the other hand, there is no such parallel mechanism (visual or contextual cues) to assess the risk of disclosure in an online environment. In a computer mediated communication, visual or contextual meta-information could be attached to a piece of information without compromising identifiabilities of information sharers. As a result, privacy risks (e.g., misrepresentation) and slips (e.g.,inadvertently sharing personal information) might be minimized.

- Reputation Exchange: The lack of trust makes privacy solutions extremely difficult and expensive. In the online world of information asymmetry it is very hard to discover a trustee. Two partners may not have necessary pieces of information about each other to make a trust-based privacy decision. Expanding on my existing work on privacy-preserving trust evaluation, I plan to develop a mechanism to exchange reputation in one domain for reputation in another domain.

- Context Facilitation (Switches): In the disembodied online world, one can assume as many identities as they wish and freely move across multiple identities to present themselves in various contexts. The users need to be informed if starting an action implies a context switch, and they must have the possibility to switch their partial identities in this case.

- Parsimonious Authentication: The need for authentication, in turn, is responses to the need to avoid or reduce the risk that the wrong person will access, use, change, or delete personal information. Authentication may require the disclosure of personal information by a user [Kent and Millett, 2003]. The proliferation of authentication activity implies more collection and circulation of personal information. Parsimonious authentication refers to finding answers to the following questions: is authentication necessary? If so, how should it be accomplished so that privacy risk is minimized?

6.7 Concluding Remarks

This thesis focused on building a privacy-preserving information sharing paradigm by addressing the potential variability in individuals' expectations of privacy. An expectation of privacy is influenced by many variables, including context and trust. In this regard, an identity and trust-based computation model for privacy (ITMP) has been constructed to preserve privacy by enabling users to control the flow and regulate the boundary and persistence of shared information. The ITMP model is instantiated in the online discussion forum of an e-learning environment and validated through user studies. Some of my initial hypothesis were substantiated and original research goals are achieved in large measure.

In conclusion, this foray into the world of privacy protection in an online world has uncovered more questions than it has answered. Privacy is indeed a complex issue. The ITMP represents an important step toward a comprehensive privacy solution.

References

[Abrams and Joyce, 1995] Abrams, M. D. and Joyce, M. V. (1995). Trusted System Concepts. Computers & Security, 14(1):45–56.

[Acquisti, 2004] Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. In EC'04.

[Acquisti and Gross, 2006] Acquisti, A. and Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In Privacy Enhancing Technologies, pages 36–58.

[Adamic, 1999] Adamic, L. A. (1999). The Small World Web. In Abiteboul, S. and Vercoustre, A.-M., editors, Proc. 3rd European Conf. Research and Advanced Technology for Digital Libraries, ECDL, number 1696, pages 443–452. Springer-Verlag.

[Agrawal et al., 2005] Agrawal, R., Srikant, R., and Thomas, D. (2005). Privacy preserving olap. In SIGMOD '05: Proceedings of the 2005 ACM SIGMOD international conference on Management of data, pages 251–262, New York, NY, USA. ACM.

[Al-Fedaghi, 2005] Al-Fedaghi, S. S. (2005). How to Calculate the Information Privacy. In PST, pages 3–13.

[Allan and Lawless, 2003] Allan, J. and Lawless, N. (2003). Stress Caused by Online Collaboration in e-Learning: A Developing Model. Education and Training, 45(8/9):564–572.

[Altman, 1975] Altman, I. (1975). The environment of Social Behavior: Privacy, Personal Space, Territory, Crowding. Brooks/Cole Publication Company.

[Altman and Chemers, 1980] Altman, I. and Chemers, M. (1980). Culture and Environment. Wadsworth Publishing Company, Stamford, CT.

[Andersson et al., 2005] Andersson, C., Camenisch, J., Crane, S., Fischer-Hubner, S., Leenes, R., Pearsorr, S., Pettersson, J., and Sommer, D. (2005). Trust in PRIME. isspit, 0:552–559.

[Anwar and Greer, 2006] Anwar, M. and Greer, J. (2006). Reputation Management in Privacy-enhanced E-learning. In Proceedings of the 3rd Annual Scientific Conference of the LORNET Research Network (I2LOR-06), Montreal, Canada.

[Anwar and Greer, 2008a] Anwar, M. and Greer, J. (2008a). Enabling reputation-based trust in privacy-enhanced learning systems. In The Proceedings of the 9th International Conference on Intelligent Tutoring Systems (ITS2008), Montreal, Canada.

[Anwar and Greer, 2008b] Anwar, M. and Greer, J. (2008b). Role- and relationship-based identity management for private yet accountable e-learning. In IFIPTM 2008: Joint iTrust and PST Conferences on Privacy, Trust management and Security, Trondheim, Norway.

[Anwar et al., 2006] Anwar, M., Greer, J., and Brooks, C. (2006). Privacy Enhanced Personlization in E-learning. In Proceedings of the 2006 International Conference on Privacy, Security, and Trust, Markham, Ontario, Canada.

[Barkley et al., 1997] Barkley, J. F., Cincotta, A. V., Ferraiolo, D. F., Gavrila, S., and Kuhn, D. R. (1997). Role Based Access Control for the World Wide Web. In Proc. 20th NIST-NCSC National Information Systems Security Conference, pages 331–340.

[Barnes, 2006] Barnes, S. B. (2006). A Privacy Paradox: Social Networking in the United States. First Monday: Peer-reviewed Journal on the Internet, 11(9).

[Bashir et al., 2001] Bashir, I., Serafini, E., and Wall, K. (2001). Securing network software applications: introduction. Commun. ACM, 44(2):28–30.

[Bell and Padula, 1976] Bell, D. E. and Padula, L. L. (1976). Secure computer system: Unified exposition and multics interpretation. Technical Report Technical Report ESD-TR-75-306, Electronics Systems Division, AFSC, Hanscom AF Base, Bedford, Massachusetts.

[Blaze et al., 1996] Blaze, M., Feigenbaum, J., and Lacy, J. (1996). Decentralized Trust Management. Technical Report 96-17.

[Blaze et al., 2003] Blaze, M., Ioannidis, J., and Keromytis, A. D. (2003). Experience with the KeyNote Trust Management System: Applications and Future Directions. In iTrust, pages 284–300.

[Borcea et al., 2005] Borcea, K., Donker, H., Franz, E., Pfitzmann, A., and Wahrig, H. (2005). Towards Privacy-Aware eLearning. In Privacy Enhancing Technologies, pages 167–178.

[Boyd, 2002] Boyd, D. (2002). Faceted Identity: Managing representation in a digital world. M.s. thesis, MIT. Donath, Judith.

[Boyd, 2004] Boyd, D. M. (2004). Friendster and publicly articulated social networking. In CHI '04: CHI '04 extended abstracts on Human factors in computing systems, pages 1279–1282, New York, NY, USA. ACM Press.

[Brierley-Newell, 1998] Brierley-Newell, P. (1998). A cross-cultural Comparison of Privacy Definitions and Functions: A Systems Approach. Journal of Environ. Psych., 18:357–371.

[Briggs et al., 2004] Briggs, P., Simpson, B., and Angeli, A. D. (2004). Personalisation and trust: a reciprocal relationship? pages 39–55.

[Brown, 2001] Brown, J. (2001). Personalize me, Baby. Salon. Retrieved July 20, 2006, from http://archive.salon.com/tech/feature/2001/04/06/personalization/index.html.

[Buffett et al., 2004] Buffett, S., Scott, N., Spencer, B., Richter, M., and Fleming, M. W. (2004). Determining Internet Users' Values for Private Information. In PST, pages 79–88.

[Cady and McGregor, 2002] Cady, G. H. and McGregor, P. (2002). Protect Your Digital Privacy: Survival Skills for the Information Age. Macmillan Computer Publishing (MCP).

[Camenisch et al., 2005] Camenisch, J., abhi shelat, Sommer, D., Fischer-Hübner, S., Hansen, M., Krasemann, H., Lacoste, G., Leenes, R., and Tseng, J. (2005). Privacy and Identity Management for Everyone. In DIM '05: Proceedings of the 2005 workshop on Digital identity management, pages 20–27, New York, NY, USA. ACM.

[Camenisch and Herreweghen, 2002] Camenisch, J. and Herreweghen, E. V. (2002). Design and implementation of the idemix anonymous credential system. In CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, pages 21–30, New York, NY, USA. ACM.

[Camenisch and Lysyanskaya, 2001] Camenisch, J. and Lysyanskaya, A. (2001). EUROCRYPT 2001, chapter An efficient system for non-transferable anonymous credentials with optional anonymity revocation, page 93118. Heidelberg: Springer.

[Cameron, 2005] Cameron, K. (2005). The Laws of Identity. Technical report, Microsoft Whitepaper. Retrieved October 5, 2007, from http://msdn.microsoft.com/en-us/library/ms996456.aspx.

[Cantor et al., 2005] Cantor, S., Kemp, J., Philpott, R., and Maler, E. (2005). Assertions and Protocols for the Oasis Security Assertion Markup Language (SAML) v2.0. Technical report. Retrieved June 12, 2006, from http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[Cave, 2005] Cave, D. (2005). 16 to 25? Pentagon has your number, and more. The New York Times.

[Cavoukian, 2002] Cavoukian, A. (2002). The Privacy Payoff. McGraw-Hill Ryerson, Toronto.

[Cavoukian, 2006] Cavoukian, A. (2006). The Privacy Imperative: Go Beyond Compliance to Competitive Advantage. Retrieved June 12, 2007, from texttthttp://www.ipc.on.ca/images/Resources/up-2006_04_11_Arizona_BusinessSchool.pdf.

[Chellappa and Sin, 2005] Chellappa, R. K. and Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. Inf. Tech. and Management, 6(2-3):181–202.

[ChoiceStream Inc., 2004] ChoiceStream Inc. (2004). Review of Personalization Technologies: Collaborative Filtering vs. ChoiceStream's Attributized Bayesian Choice Modeling. Retrieved January 6, 2007, from http://www.choicestream.com/pdf/ChoiceStream_TechBrief.pdf.

[ChoiceStream Inc., 2006] ChoiceStream Inc. (2006). Choicestream Personalization Survey: Consumer Trends and Perceptions. Retrieved January 6, 2007, from http://www.choicestream.com/pdf/ChoiceStream_PersonalizationSurveyResults2006.pdf.

[Chu, Y., 1997] Chu, Y. (1997). REFEREE: Trust Management for Web Applications. Retrieved October 16, 2006, from http://www.w3.org/PICS/TrustMgt/presentation/97-04-08-referee-www6/.

[Cranor, 1999] Cranor, L. F. (1999). Internet Privacy. Commun. ACM, 42(2):28–38.

[Cranor, 2003] Cranor, L. F. (2003). 'i didn't buy it for myself': Privacy and ecommerce personalization. In ACM Workshop on Privacy in the Electronic Society, Washington, DC.

[Culnan, 2000] Culnan, M. J. (2000). Protecting Privacy Online: Is Self-regulation Working? Journal of Public Policy & Marketing, 19(1):2026.

[Dagger et al., 2003] Dagger, D., Wade, V., and Conlan, O. (2003). Towards "anytime, anywhere" Learning: The Role and Realization of Dynamic Terminal Personalization in Adaptive eLearning. In Proceedings of the World Conference on Educational Multimedia, Hypermedia and Telecommunications (Ed-Media 03), pages 32–35, Chesapeake, VA.

[Dalenius, 1986] Dalenius, T. (1986). Finding a Needle in a Haystack or Identifying Anonymous Census Record. Journal of Official Statistics, 2(3):329–336.

[Demchak and Fenstermacher, 2004] Demchak, C. C. and Fenstermacher, K. D. (2004). Balancing Security and Privacy in the Information and Terrorism Age: Distinguishing Behavior from Identity Institutionally and Technologically. The Forum, 2(2).

[Department of Justice, 2000] Department of Justice, C. (2000). The Personal Information Protection and Electronic Documents Act (PIPEDA). Electronic Version.

[Dimitrakos, 2002] Dimitrakos, T. (2002). A Service-Oriented Trust Management Framework. In Trust, Reputation, and Security, pages 53–72, Heidelberg. Springer.

[Donath, 1998] Donath, J. S. (1998). Identity and Deception in the Virtual Community. In Kollock, P. and Smith, M., editors, Communities in Cyberspace. Routledge, London.

[Doney and Cannon, 1997] Doney, P. M. and Cannon, J. P. (1997). An Examination of the Nature of Trust in Buyer-seller Relationships. Journal of Marketing, 61:35–51.

[Dourish and Anderson, 2006] Dourish, P. and Anderson, K. (2006). Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. Human-Computer Interaction, 21:319–342.

[Downes, 2005] Downes, S. (2005). E-learning 2.0. eLearn, 2005(10):1.

[El-Khatib et al., 2003] El-Khatib, K., Korba, L., Xu, Y., and Yee, G. (2003). Privacy and Security in ELearning. International Journal of Distance Education Technologies, 1(4).

[Ellison and Schneier, 2000] Ellison, C. and Schneier, B. (2000). Ten risks of PKI: what you're not being told about Public Key Infrastructure. Computer Security Journal, 16(1):1–7.

[EU, 2002] EU (2002). Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.

[Feenberg, 1989] Feenberg, A. (1989). The Written World: On the Theory and Practice of Computer Conferencing. In Mason, R. and Kaye, A., editors, Mindweave: communication, computers and distance education, pages 22–39. Pergamon Press, Oxford.

[Franz et al., 2006] Franz, E., Liesebach, K., and Borcea-Pfitzmann, K. (2006). Privacy-aware User Interfaces within Collaborative Environments. In CAI '06: Proceedings of the international workshop in conjunction with AVI 2006 on Context in advanced interfaces, pages 45–48, New York, NY, USA. ACM.

[Friedman et al., 2000] Friedman, B., Peter H. Khan, J., and Howe, D. C. (2000). Trust Online. Commun. ACM, 43(12):34–40.

[Gabber et al., 1999] Gabber, E., Gibbons, P. B., Kristol, D. M., Matias, Y., and Mayer, A. (1999). Consistent, yet Anonymous, Web Access with LPWA. Commun. ACM, 42(2):42–47.

[Gavison, 1984] Gavison, R. (1984). Privacy and the Limits of Law. In Schoeman, F., editor, Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press, New York, NY.

[Gerck, 1998] Gerck, E. (1998). Overview of Certification Systems: X.509, CA, PGP and SKIP.

[Goffman, 1959] Goffman, E. (1959). The Presentation of Self in Everyday Life. Anchor.

[Golbeck and Hendler, 2004] Golbeck, J. and Hendler, J. (2004). Accuracy of Metrics for Inferring Trust and Reputation in Semantic Web-Based Social Networks. In Engineering Knowledge in the Age of the SemanticWeb, volume 3257, pages 116–131.

[Goldberg and Shostack, 2001] Goldberg, I. and Shostack, A. (2001). Freedom Network 1.0 Architecture and Protocols. Technical report, Freedom Network. Retrieved April 5, 2007, from http://www.homeport.org/ adam/zeroknowledgewhitepapers/arch-tech.pdf.

[Goldberg et al., 1997] Goldberg, I., Wagner, D., and Brewer, E. (1997). Privacy-enhancing Technologies for the Internet. In COMPCON '97: Proceedings of the 42nd IEEE International Computer Conference, page 103, Washington, DC, USA. IEEE Computer Society.

[Goldschlag et al., 1999] Goldschlag, D., Reed, M., and Syverson, P. (1999). Onion Routing for Anonymous and Private Internet Connections. Communications of the ACM (USA), 42(2):39–41.

[Grandison and Sloman, 2000] Grandison, T. and Sloman, M. (2000). A survey of trust in internet applications. IEEE Communications Surveys and Tutorials, 3(4).

[Gross and Acquisti, 2005] Gross, R. and Acquisti, A. (2005). Privacy and Information Revelation in Online Social Networks. In Proceedings of the ACM CCS Workshop on Privacy in the Electronic Society (WPES '05).

[Grudin, 2001] Grudin, J. (2001). Desituating Action: Digital Representation of Context. Human-Computer Interaction, 16(2):269–286.

[Handy, 1999] Handy, C. (1999). Trust and the Virtual Organization. pages 107–120.

[Holtzman, 2006] Holtzman, D. H. (2006). Privacy Lost: How Technology Is Endangering Your Privacy. Jossey-Bass Inc., Publishers.

[Jaquet-Chiffelle et al., 2006] Jaquet-Chiffelle, D., Benoist, E., and Anrig, B. (2006). Identity in a Networked World Use Cases and Scenarios. Technical report, FIDIS. http://www.fidis.net/fileadmin/fidis/deliverables/fidiswp2-del2.6_Identity_in_a_Networked_World.pdf.

[Johnson and Miller, 1998] Johnson, D. G. and Miller, K. (1998). Anonymity, Pseudonymity, or Inescapable Identity on the Net (abstract). SIGCAS Comput. Soc., 28(2):37–38.

[Jøsang et al., 2007] Jøsang, A., Zomai, M. A., and Suriadi, S. (2007). Usability and Privacy in Identity Management Architectures. In ACSW '07: Proceedings of the fifth Australasian symposium on ACSW frontiers, pages 143–152, Darlinghurst, Australia, Australia. Australian Computer Society, Inc.

[Joshi et al., 2001] Joshi, J. B. D., Aref, W. G., Ghafoor, A., and Spafford, E. H. (2001). Security Models for Web-based Applications. Commun. ACM, 44(2):38–44.

[Kent and Millett, 2002] Kent, S. T. and Millett, L. I. (2002). IDs Not That Easy: Questions About Nationwide Identity Systems. Technical report, Committee on Authentication Technologies and Their Privacy Implications, National Research Council. http://www.nap.edu/books/030908430X/html/.

[Kent and Millett, 2003] Kent, S. T. and Millett, L. I., editors (2003). Who Goes There? Authentication Through the Lens of Privacy. National Academy Press, Washington, D.C. US National Research Council.

[Kobsa, 2007] Kobsa, A. (2007). Privacy-enhanced web personalization. pages 628–670.

[Kobsa and Schreck, 2003] Kobsa, A. and Schreck, J. (2003). Privacy through Pseudonymity in User-adaptive Systems. ACM Trans. Inter. Tech., 3(2):149–183.

[Kumar, 2006] Kumar, V. (2006). Trust and Security in Peer-to-Peer System. In DEXA '06: Proceedings of the 17th International Conference on Database and Expert Systems Applications, pages 703–707, Washington, DC, USA. IEEE Computer Society.

[Lessig, 1999] Lessig, L. (1999). The Architecture of Privacy. Vanderbilt Entertainment Law and Practice, 1:56–65.

[Lilien and Bhargava, 2006] Lilien, L. and Bhargava, B. K. (2006). A Scheme for Privacy-preserving Data Dissemination. IEEE Transactions on Systems, Man, and Cybernetics, Part A, 36(3):503–506.

[Luhmann, 2000] Luhmann, N. (2000). Familiarity, Confidence, Trust: Problems and Alternatives. In Gambetta, G., editor, Trust:Making and Breaking Cooperative Relations, pages 94–107. Oxford.

[Machanavajjhala et al., 2007] Machanavajjhala, A., Gehrke, J., Kifer, D., and Venkitasubramaniam, M. (2007). ℓ-diversity: Privacy beyond κ-anonymity. ACM Transaction on Knowledge Discovery from Data, 1(1):3.

[Maes, 2005] Maes, P. (2005). Interestmap: Harvesting social network profiles for recommendations. Beyond Personalization.

[Maler and Reed, 2008] Maler, E. and Reed, D. (2008). The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Security and Privacy, 6(2):16–23.

[Marsh, 1994] Marsh, S. P. (1994). Formalizing Trust as a Computational Concept. PhD thesis, Department of Computer Science and Mathematics, University of Stirling, UK.

[Mason and Lefrere, 2003] Mason, J. and Lefrere, P. (2003). Trust, Collaboration, and Organisational Transformation. International Journal of Training and Development, 7(4):259–271.

[Mayer et al., 1995] Mayer, R. C., Davis, J. H., and Schoorman, D. F. (1995). An Integrative Model of Organizational Trust. Academy ol Management Review, 20(3):709–734.

[McCalla, 2000] McCalla, G. (2000). The Fragmentation of Culture, Learning, Teaching and Technology: Implications for the Artificial Intelligence in Education Research Agenda in 2010. International Journal of Artificial Intelligence in Education, pages 177–196.

[McCalla et al., 2000] McCalla, G. I., Vassileva, J., Greer, J. E., and Bull, S. (2000). Active Learner Modelling. In ITS '00: Proceedings of the 5th International Conference on Intelligent Tutoring Systems, pages 53–62, London, UK. Springer-Verlag.

[Menard, 2006] Menard, M. C. (2006). Privacy Protection for E-Services, chapter Privacy Protection through Security. IGI Publishing.

[Merrells, 2004] Merrells, J. (2004). XACML: XML Access Control. Retrieved January 16, 2007 from `http://www.idealliance.org/papers/dx_xmle04/papers/04-01-04/04-01-04.pdf`.

[Mont, 2004] Mont, M. C. (2004). Dealing with Privacy Obligations: Important Aspects and Technical Approaches. In TrustBus, pages 120–131.

[Mont et al., 2003] Mont, M. C., Pearson, S., and Bramhall, P. (2003). Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services. dexa, 00:377.

[Nanda, 2007] Nanda, A. (2007). Identity Selector Interoperability Profile 1.0. Technical report, Microsoft Inc. Retrieved May 1, 2008, from `http://download.microsoft.com/download/1/1/a/11ac6505-e4c0-4e05-987c-6f1d31855cd2 Identity-Selector-Interop-Profile-v1.pdf`.

[Neuhold, 2003] Neuhold, E. J. (2003). Personalization and User profiling & Recommender Systems. In Proceedings of the WI/IM Information management Proseminar.

[Nichani, 2000] Nichani, M. R. (2000). Learning through social interactions (online communities). Elearningpost. Retrieved January 12, 2007, from `http://www.elearningpost.com/elthemes/comm.pdf`.

[Nissenbaum, 2004] Nissenbaum, H. F. (2004). Privacy as Contextual Integrity. Washington Law Review, 79(1):119–158.

[Noam, 1997] Noam, E. (1997). Privacy and Self-Regulation: Markets for Electronic Privacy. Technical report, U.S. Dept. of Commerce. http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1B.

[Palen and Dourish, 2003] Palen, L. and Dourish, P. (2003). Unpacking "Privacy" for a Networked World. In CHI'03.

[Patil and Kobsa, 2003] Patil, S. and Kobsa, A. (2003). The Challenges in Preserving Privacy in Awareness Systems(ISR Technical Report No. UCI-ISR-03-3). Technical report, Institute for Software Research, Irvine, CA, USA.

[Patil and Kobsa, 2005] Patil, S. and Kobsa, A. (2005). Designing with privacy in mind. In Proceedings of CHI-2005 Workshop on Awareness Systems : Known Results, Theory, Concepts and Future Challenges.

[Patrick, 2002] Patrick, J. R. (2002). Net Attitude: What it is, How to get it, and Why Your Company Can't Survive Without It, chapter Trusted, page 151. Perseus Books Group.

[Personalization Consortium, 2005] Personalization Consortium (2005). Retrieved March 5, 2007, from `www.personalization.org/personalization.html`.

[Raghu et al., 2001] Raghu, T. S., Kannan, P. K., Rao, H. R., and Whinston, A. B. (2001). Dynamic Profiling of Consumers for Customized Offerings over the Internet: a Model and Analysis. Decision Support Systems, 32(2):117–134.

[Rao and Rohatgi, 2000] Rao, J. R. and Rohatgi, P. (2000). Can Pseudonymity Really Guarantee Privacy? In Proceedings of the Ninth USENIX Security Symposium, pages 85–96. USENIX.

[Recordon and Reed, 2006] Recordon, D. and Reed, D. (2006). OpenID 2.0: A Platform for User-centric Identity Management. In DIM '06: Proceedings of the second ACM workshop on Digital identity management, pages 11–16, New York, NY, USA. ACM Press.

[Reiter and Rubin, 1999] Reiter, M. K. and Rubin, A. D. (1999). Anonymous Web Transactions with Crowds. Communications of the ACM, 42(2):32–48.

[Rezgui et al., 2003] Rezgui, A., Bouguettaya, A., and Malik, Z. (2003). A Reputation-based Approach to Preserving Privacy in Web Services. In Proceedings of the 4th International Workshop on Technologies for E-Services, pages 91–103.

[Ridings and Shishigin, 2002] Ridings, C. and Shishigin, M. (2002). Pagerank Uncovered. Technical report. textttthttp://www.voelspriet2.nl/PageRank.pdf.

[Rust and Kannan, 2003] Rust, R. T. and Kannan, P. K. (2003). E-service: a new paradigm for business in the electronic environment. Commun. ACM, 46(6):36–42.

[Samarati, 2001] Samarati, P. (2001). Protecting Respondents' Identities in Microdata Release. IEEE Transactions on Knowledge and Data Engineering, 13(6):1010–1027.

[Sartor, 2006] Sartor, G. (2006). Privacy, Reputation, and Trust: Some Implications for Data Protection. EUI-LAW Working Papers 4, European University Institute (EUI), Department of Law. Retrieved December 15, 2006, from at http://ideas.repec.org/p/erp/euilaw/p0040.html.

[Shardanand and Maes, 1995] Shardanand, U. and Maes, P. (1995). Social Information Filtering: Algorithms for Automating Word of Mouth. In Proc. ACM Conf. Human Factors in Computing Systems (CHI 95), page 210217. ACM Press.

[Sheehan and Hoy, 2000] Sheehan, K. B. and Hoy, M. G. (2000). Dimensions of Privacy Concern among Online Consumers. Journal of Public Policy & Marketing, 19(1):62–73.

[Solove, 2006] Solove, D. J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review, 154(3):477.

[Song et al., 2006] Song, R., Korba, L., and Yee, G. (2006). Pseudonym Technology for E-Services. In Privacy Protection for E-Services, edited by G. Yee,.

[Steel, 1991] Steel, J. L. (1991). Interpersonal Correlates of Trust and Self-Disclosure. Psychological Reports, 68:1319–1320.

[Sweeney, 2002] Sweeney, L. (2002). k-anonymity: A Model for Protecting Privacy. International journal of uncertainty, fuzziness, and knowledge-based systems.

[Teltzrow and Kobsa, 2004] Teltzrow, M. and Kobsa, A. (2004). Impacts of User Privacy Preferences on Personalized Systems: a Comparative Study. pages 315–332.

[USACM, 2006] USACM (2006). USACM Policy Recommendations on Privacy. Retrieved June 17, 2007, from http://usacm.acm.org/usacm/Issues/Privacy.htm.

[Ventuneac et al., 2003] Ventuneac, M., Coffey, T., and Salomie, I. (2003). A Policy-based Security Framework for Web-enabled Applications. In ISICT '03: Proceedings of the 1st international symposium on Information and communication technologies, pages 487–492. Trinity College Dublin.

[Volokh, 2000] Volokh, E. (2000). Personalization and Privacy. Commun. ACM, 43(8):84–88.

[Wang and Kobsa, 2008] Wang, Y. and Kobsa, A. (2008). Handbook of Research on Social and Organizational Liabilities in Information Security. chapter Privacy-Enhancing Technologies. Idea Group Inc. Global.

[Wang and Vassileva, 2003] Wang, Y. and Vassileva, J. (2003). Trust and reputation model in peer-to-peer networks. In Third International Conference on Peer-to-Peer Computing, (P2P 2003), pages 150–157.

[Warren and Brandeis, 1890] Warren, S. and Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, IV(5).

[Weitzner, 2007] Weitzner, D. J. (2007). Whose Name Is It, Anyway? Decentralized Identity Systems on the Web. IEEE Internet Computing, 11(4):72–76.

[Westin, 1967] Westin, A. F. (1967). Privacy and Freedom. Atheneum, New York, NY.

[White, 2004] White, M. (2004). Access Control in Smart Space Environments. Technical report, M-Zones White Paper, Ireland.

[Windley, 2005] Windley, P. (2005). Digital Identity. O'Reilly Media, Inc.

[Wu and Weaver, 2005] Wu, Z. and Weaver, A. C. (2005). A Privacy Preserving Enhanced Trust Building Mechanism for Web Services. In PST.

[Xu and Korba, 2002] Xu, Y. and Korba, L. (2002). A Trust Model for Distributed E-Learning Service Control. In In G. Richards (Ed.), proceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, pages 2419–2434, Chesapeake, VA.

[Yang and Padmanabhan, 2005] Yang, Y. and Padmanabhan, B. (2005). The evaluation of online personalization systems: A survey of evaluation schemes and a knowledge-based approach. Journal of Electronic Commerce Research, 6(2):112–120.

[Yao et al., 2007] Yao, M. Z., Rice, R. E., and Wallis, K. (2007). Predicting User Concerns about Online Privacy. Journal of the American Society for Information Science and Technology, 58(5):710–722.

[Young, 1978] Young, J. (1978). Introductions: A Look at Privacy, chapter Privacy. Wiley.

[Yuan and Tong, 2005] Yuan, E. and Tong, J. (2005). Attributed Based Access Control (ABAC) for Web Services. In ICWS '05: Proceedings of the IEEE International Conference on Web Services (ICWS'05), pages 561–569, Washington, DC, USA. IEEE Computer Society.

[Zimmermann, 1994] Zimmermann, P. (1994). PGP Users Guide, Volume 1: Essential Topics,. Boulder Software Engineering,, 3021 Eleventh Street, Boulder, Colorado 80304, USA,.

Appendix A

Screen Shots of Privacy-augmented iHelp Discussion from Larger-scale Study

Figure A.1: iHelp Discussion Context Window

Figure A.2: iHelp Discussion Partial Identities Window

User Aliases

Current aliases:

Category	Alias
User-level Aliases	M Anwar(moa060) *(default)*
	abc
	dont care
Apathetic	Apathetic#
	CareFree
	Yo
DeepThinkerIntellectual	Intellectual#
	Sage
DevilsAdvocate	Devil#
	asd
EnvironmentalistActivist	Activist#
	Suzuki
Luddite	Luddite#
MissCongeniality	Congeniality#
RightwingConservative	Conservative#
	Bush
Sexist	Sexist#
	Hotty
	Man

Actions:

- Create new alias

Figure A.3: iHelp Discussion Partial Identity Creation Window

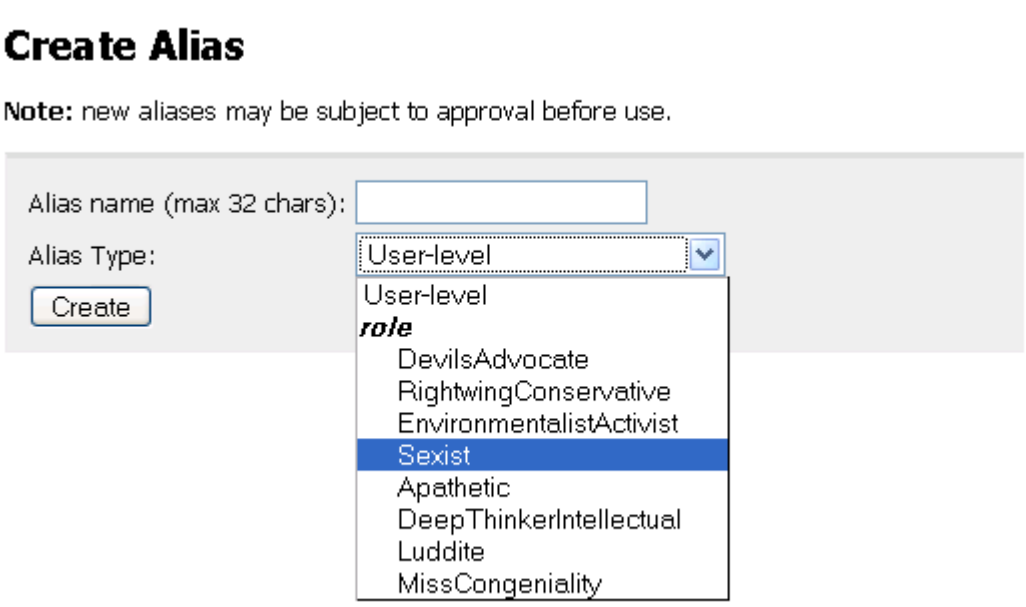


Figure A.4: iHelp Discussion Messagelist Window

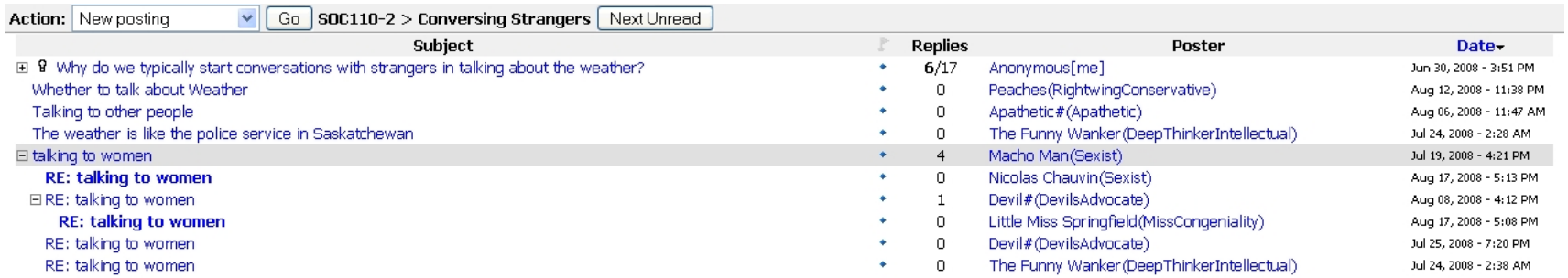


Figure A.5: iHelp Discussion Message Window

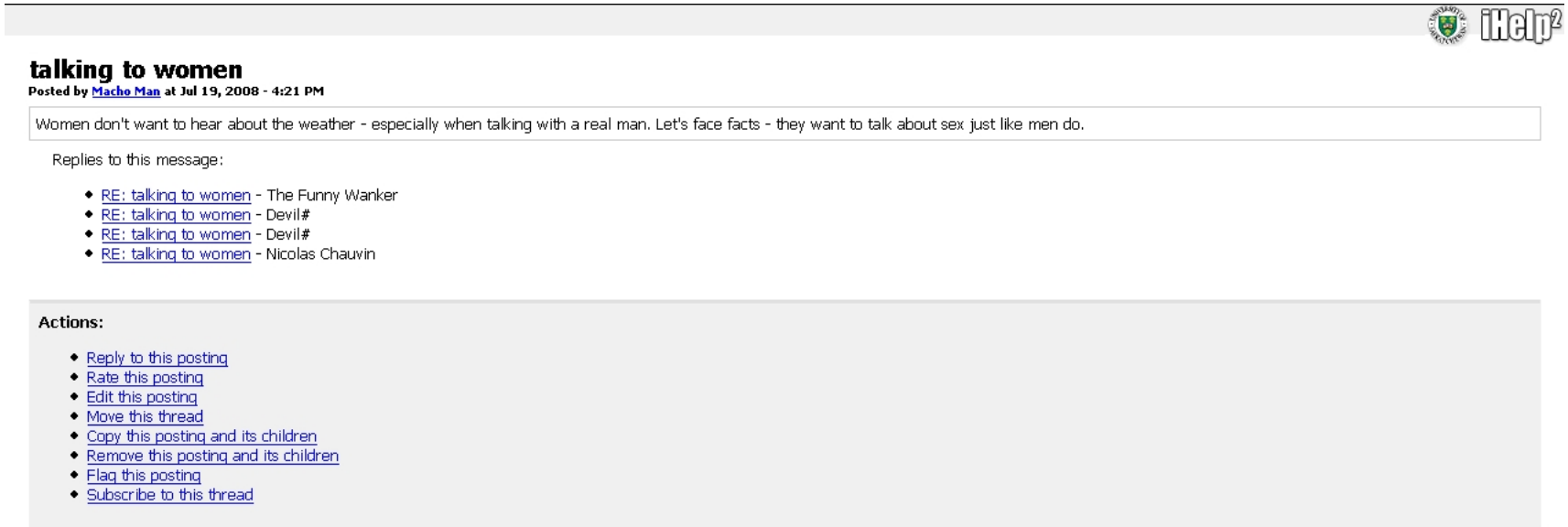


Figure A.6: iHelp Discussion Reply Window

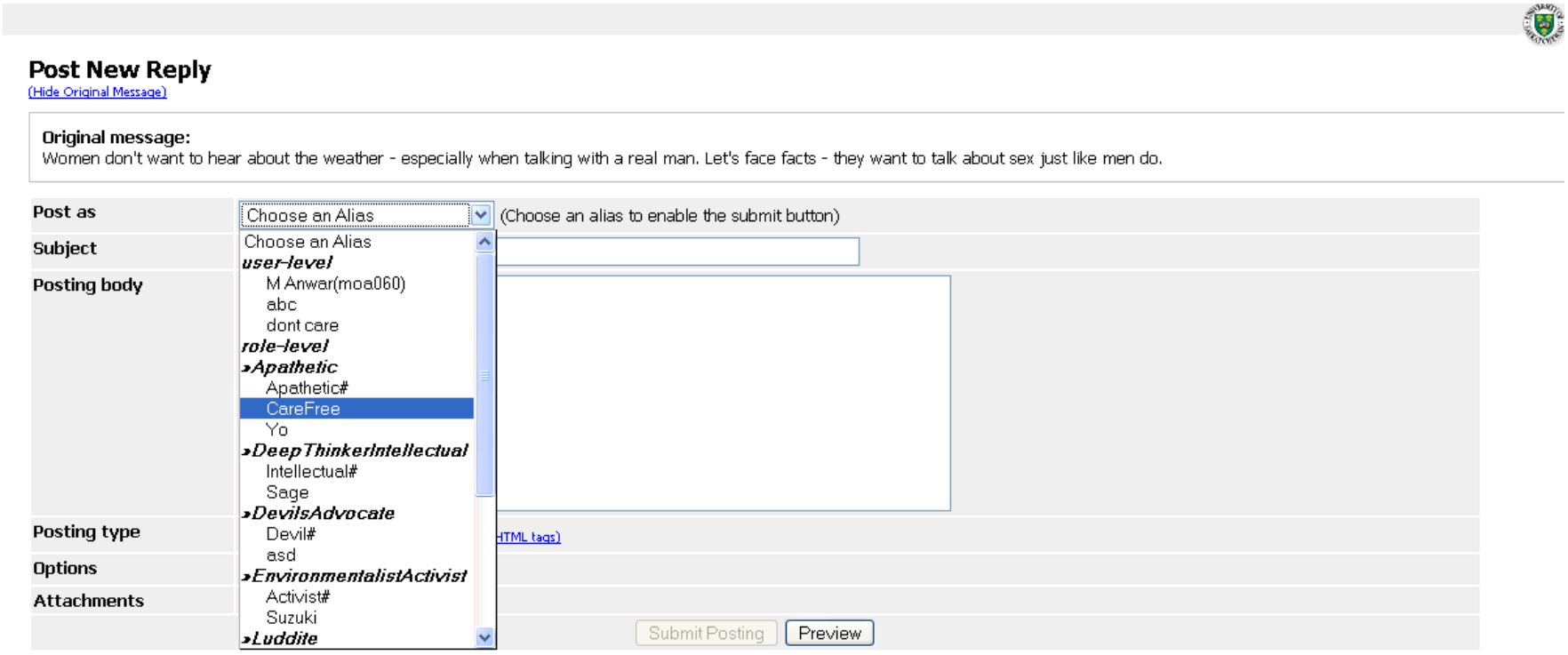
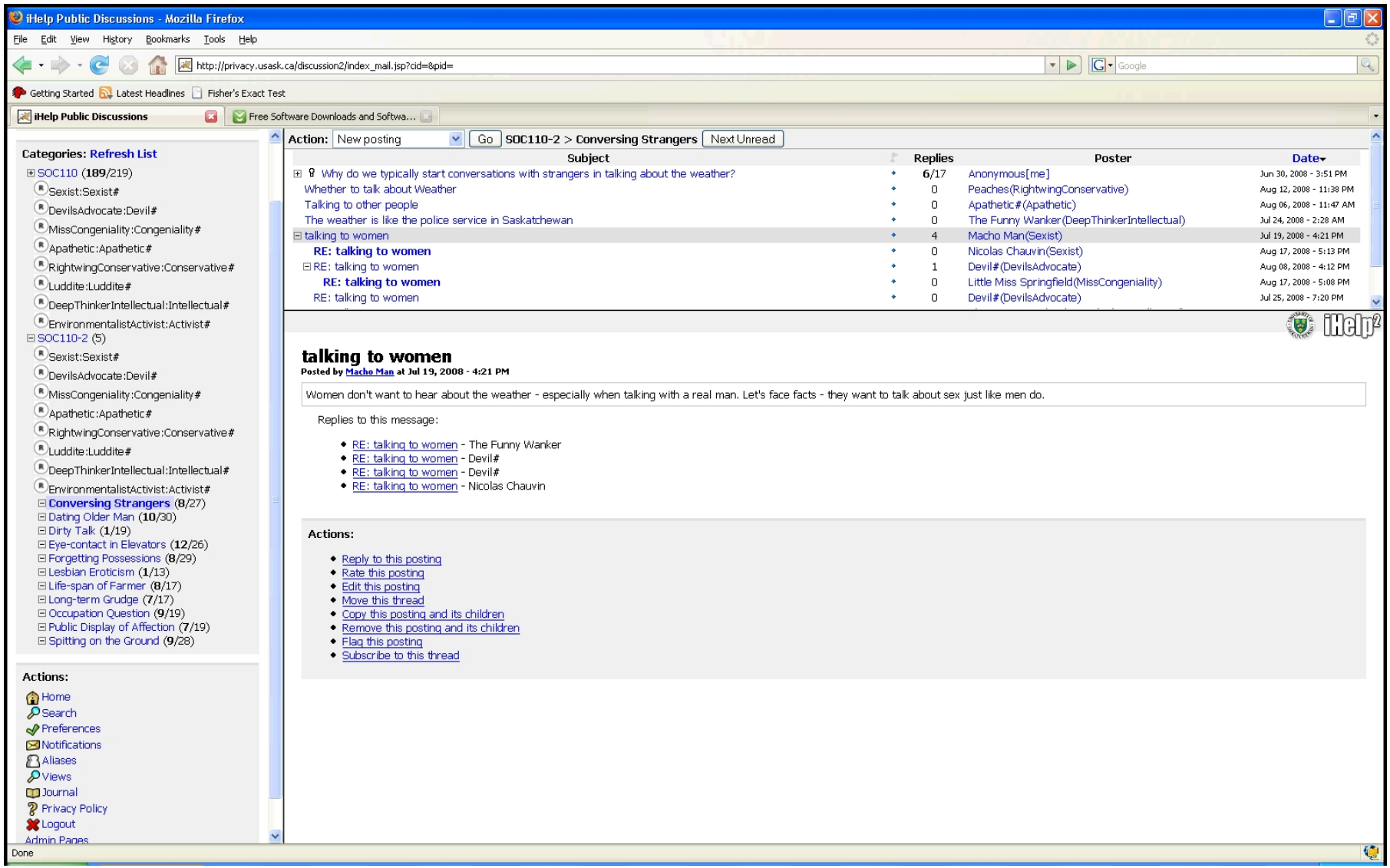


Figure A.7: iHelp Discussion Reputation Window

Figure A.8: iHelp Discussion Main Window



Appendix B

Study Consent Form

Consent Form
Approved by the University of Saskatchewan Advisory Committee on Ethics in Behavioural Sciences Research (BSC# 2001-198)

1. **Title of the study.**
   I-Help: A preliminary Evaluative Study
   Role- and Relationship-based Identity Management in iHelp Discussion

2. **Name(s), institutional affiliation(s) and telephone number(s) of researchers.**
   Jim Greer, Professor, Computer Science Department; 966-8655
   Mohd Anwar, PhD Student, Computer Science Department

3. **Purpose and objectives of the study.**

This is an experimental study of on-line instructional support. This study is part of the research being conducted by the ARIES Group at the University of Saskatchewan, Department of Computer Science.
The goal of the study is:

- **To support privacy-enhanced online learning environment**
- **To evaluate the effectiveness of Role- and Relationship-based Identity Management in offering privacy and facilitating trust building**

4. **The possible benefits to the participants** will be an improved learner support environment for future users of the I-Help system.

5. **Data Collection Procedure**

   Your activities in using the I-Help computer system will be logged. You are asked to use the system normally (as you would in support of your normal coursework). In addition, for this study we ask you specifically to:

   - **Fill out an online post-use survey to reflect upon your use experience of the new version of iHelp Discussion Forum with privacy-preserving and trust-facilitating features**

   The survey should take approximately **30** minutes.

6. **Risks or Side Effects**
   It is hard to envisage any risks or side effects of the usage of the system. However, if we become aware of any such effects during the study, we will inform immediately the participants.

7. **Each participant is free to withdraw** from the study at any time and this withdrawal will not affect the participants' academic status. If appropriate, the researcher may choose to discontinue a participant's involvement in the study. In any case data related to students who withdraw will be deleted from the study and destroyed.

8. **The information about the students** The student models as well as the contents of communication among the students and with helpers will be stored within the system and will not be available to anyone except for the researchers involved in the project.

9. **The anonymity** of the collected data and the privacy of the subjects would be completely protected and the information obtained from this data would be used only in theses, journal articles or conference publications written by the researchers. In any publication only aggregate data will be reported. Thus, the names and identities of the subjects would not be published in any form.

10. **The participants will be advised** of any new information that will have a bearing on the participants' decision to continue in the study.

11. If you want to acquire information on the results of the research once the study is completed, send a request to **Mohd Anwar (mohd.anwar@usask.ca).**

12. Should you have any questions with regard to the study or to your rights as a participant in the research study, call Professor Jim Greer, 966-8655.

The study and contents of the consent have been explained to me, I understand the contents, and that I may receive a copy of the consent form for my own records.

Date: July 21, 2008

Signatures: _____ _____

Participant Researcher

Appendix C

Survey Questionaire from Pilot Study

Preview of Survey: Post-Use Survey of Privacy-enhanced iHelp Discussion Tool

Page 3 of 9

1. [Required] Please enter your nsid:

(255 chars max)

2. [Required] I was satisfied with the overall level of privacy protection offered me in this version of iHelp discussions

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

3. [Required] The system was inobtrusive and did not hinder my intended way of communication

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

4. [Required] I was satisfied with my ability to maintain privacy while sharing my views

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

5. [Required] I felt in control of my identity choices (which identity to use in which communication episode)

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

6. [Required] I was satisfied with the way the system enabled me to manage how I disclosed my identity

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

Quit - Do not save answers | << Previous Page | Next Page >>

UNIVERSITY OF SASKATCHEWAN

Preview of Survey: Post-Use Survey of Privacy-enhanced iHelp Discussion Tool

Page 4 of 9

7. [Required] The reputation score helped me find trustworthy people with whom to discuss issues.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

8. [Required] The system enabled me to act more candidly using my partial identities than I would have done when using a single monolithic identity

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

9. [Required] I more often read/replied to a posting by a person with a higher reputation than a posting by someone of an unknown or lower reputation

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

Quit - Do not save answers | << Previous Page | Next Page >>

10. [Required] I found the identity management features of iHelp easy to use

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

11. [Required] I found the system easy to learn

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

12. [Required] The system helped me to maintain my privacy

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

13. [Required] The system helped me to identify which postings could be trusted (by competent/benevolent/honest people)

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

14. [Required] The system facilitates trust

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

15. [Required] The system helped me to create context-sensitive identities

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

16. [Required] The system helped to safely disclose information about myself and my beliefs

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

17. the system helped me to be aware of the context of a communication episode

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

18. taking on a role helped me reveal information selectively in a communication episode

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

19. [Required] The system helped me to keep in mind the purpose of a communication episode

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

20. [Required] I tend to reply more often to a poster with a good reputation

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

21. [Required] I tend pay more attention to a poster with a good reputation

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

22. [Required] I tend to rate postings with a purpose to reward or punish/discipline the person who made the posting

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

25. [Required] The system helped me remain aware of my assumed identity

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

26. [Required] I was able to keep track of which postings were mine and which postings came from others

- Always
- Often
- Sometimes
- Rarely
- Never

27. [Required] When I took on a particular identity, I was aware of the expected behavior that may be associated with that identity

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

28. I tried to maintain integrity for good reputation

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

29. [Required] I was able to link postings (that is, I was able to identify different postings that seemed to come from the same person regardless of the identity they took on).

- Always
- Often
- Sometimes
- Rarely
- Never

30. [Required] In the discussions associated with this study, my best guess of the number of different actual people who participated would be _____.

(255 chars max)

31. [Required] I could identify which postings belonged to which actual users - even across contexts

- Always
- Often
- Sometimes
- Rarely
- Never

32. [Required] I was more authentic in my postings than I would have been had I been forced to use my true public identity

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

33. I was more direct in terms of language and phrasing than I would have been while using my public identity

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

34. [Required] I used a group identity when I wanted to rant or experience an emotional release

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

35. [Required] Because I could control the exposure of my identity, I was less guarded in my communication

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

36. At times, I played devil's advocate

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

37. I was intentionally provocative

- Always
- Often
- Sometimes
- Rarely

- Never

38. I experimented with my identity (e.g. through playing multiple roles)

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

39. Do you have any additional comments about the system?

(4000 chars max)

Appendix D

Survey Questionaire from Larger-scale Study

Please enter your nsid: _____	
Circle the number of your response 1=strongly agree 3 = neutral 5 = strongly disagree	
1. I was satisfied with the overall level of privacy protection offered to me in the 2nd version of the iHelp discussion forum	1 2 3 4 5
2. The iHelp system was in-obtrusive and did not hinder my intended way of communication	1 2 3 4 5
3. I was satisfied with my ability to maintain privacy while sharing my views	1 2 3 4 5
4. I felt in control of my identity choices (which alias to use in which communication episode)	1 2 3 4 5
5. I was satisfied with the way the system enabled me to manage how I disclosed my identity (nsid, default alias, self-created alias)	1 2 3 4 5
6. The reputation score helped me find trustworthy people with whom to discuss issues	1 2 3 4 5
7. The system enabled me to act more candidly using my partial identities (in version 2) than I would have done when using a single "real" identity (in version 1)	1 2 3 4 5
8. I value a posting by a person with a higher reputation **more** than a posting by someone of an unknown or lower reputation	1 2 3 4 5
9. I found the features of the iHelp system easy to use	1 2 3 4 5
10. I found the iHelp system easy to learn	1 2 3 4 5
11. The system helped me to maintain my privacy	1 2 3 4 5
12. The system helped me to identify which postings could be trusted (by competent/benevolent/honest people)	1 2 3 4 5
13. The system facilitates trust	1 2 3 4 5
14. The system helped me communicate appropriately in a context	1 2 3 4 5
15. The system helped to safely disclose information about myself and my beliefs	1 2 3 4 5
16. The system helped me to be aware of the context of a communication episode	1 2 3 4 5
17. I tend to reply more often to a poster with a good reputation	1 2 3 4 5

18. I tend pay more attention to a poster with a good reputation	1 2 3 4 5
19. I tend to rate postings with a purpose to reward or punish/discipline the person who made the posting	1 2 3 4 5
20. I am willing to be more open when I reply to a posting from a person with a good reputation	1 2 3 4 5
21. I tend to spend more time in reading and replying to a quality posting	1 2 3 4 5
22. The system helped me remain aware of my assumed identity (chosen through an alias)	1 2 3 4 5
23. I was able to keep track of which postings were mine and which postings came from others	1 2 3 4 5
24. When I took on a particular identity (e.g. Miss Congeniality), I was aware of the expected behavior that may be associated with that identity	1 2 3 4 5
25. I was able to link postings (that is, I was able to identify different postings that seemed to come from the same person regardless of the identity (alias) they took on).	1 2 3 4 5
26. I was more authentic in my postings than I would have been had I been forced to use my true public identity (as in version 1)	1 2 3 4 5
27. I was more direct in terms of language and phrasing than I would have been while using my true public identity (as in version 1)	1 2 3 4 5
28. I used a group identity (e.g., Devil#) when I wanted to rant or experience an emotional release	1 2 3 4 5
29. I was intentionally provocative because of available identity (alias) choices	1 2 3 4 5
Do you have any additional comments about the system?	